

IP-fähige Anwendungen in der Sicherheitstechnik: Integration in bestehende Netze

Von Stephan Holzem, Mönchengladbach

Der Einsatz von Datennetzwerken findet nicht nur in Industriebetrieben eine immer größere Verbreitung. Netzwerke werden heute sowohl zur lokalen Vernetzung von Computern als auch immer häufiger zur Kommunikation in Unternehmensverbänden genutzt oder sie sind an öffentliche Netze angebunden. Dabei kommunizieren heute nicht nur Computer über TCP/IP Datennetze. Die Anbindung von Systemen der Haustechnik ist inzwischen eine Standardanwendung. Ist ein Datennetz einmal vorhanden, erweist sich dieses als äußerst hochwertige und preiswerte Möglichkeit des Datenaustausches angeschlossener Systeme. Diese Anwendungsmöglichkeit ist auch den Herstellern sicherheitstechnischer Komponenten und Systeme nicht entgangen. Insbesondere bei den Gewerken Übertragungstechnik, Zutrittskontrolle und Videotechnik besteht heute die Möglichkeit der problemlosen Integration in Datennetze. Hieraus lassen sich erhebliche Einsparungen bei Installation und Betrieb von Leitungsnetzen erzielen.

Bei der Integration sicherheitstechnischer Systeme in reine Datennetze gilt es, Netzbesonderheiten zu berücksichtigen, um die geforderten Bedürfnisse an Datensicherheit zu erfüllen. Grundsätzlich zu unterscheiden sind „lokale Datennetze mit geschlossener Benutzergruppe“ und „Netze mit Anbindung / Übertragung an öffentliche Netze bzw. Netze ohne geschlossene Benutzergruppe“.

Auch bei der zu integrierenden Anwendung gilt es Unterschiede in Bezug auf das Gefährdungsrisiko zu beachten. Während die Übertragung von Videobildern in lokalen Netzen normalerweise keine besonderen Schutzmaßnahmen im Hinblick auf Datensicherheit erfordert, ist der Einsatz zusätzlicher Sicher-

heitsmaßnahmen bei einer Alarmübertragung über öffentliche Netze unabdingbar. Hier ist durch geeignete Maßnahmen sicherzustellen, dass die sicherheitstechnischen Daten nicht erkannt, mitgelesen oder gar verändert werden können. Zur Sicherstellung dieser Forderungen sind heute entsprechende Produkte mit integrierten SW-Modulen zur Bildung eines Virtual Private Networks am Markt verfügbar. Auf jeden Fall sollte bei der Produktauswahl darauf geachtet werden, dass die eingesetzten Produkte von entsprechenden Stellen (VdS Schadenverhütung GmbH, BSI - Bundesamt für Sicherheit in der Informationstechnologie) für die spezielle Anwendung geprüft sind.

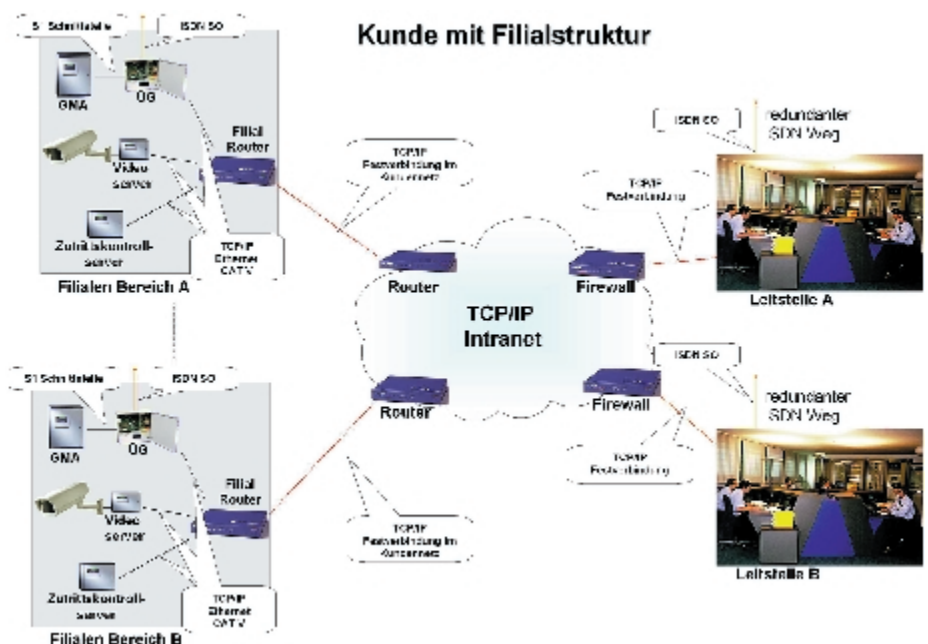
Anwendungsbeispiel „Kreditinstitut mit Filialen“:

Sämtliche Filialen sind über ein TCP/IP-Daten-

netz vernetzt. Aufgrund aufwändiger Schutzmaßnahmen im Netz und einer geschlossenen Benutzergruppe kann im Allgemeinen auf zusätzliche Sicherungsmaßnahmen verzichtet werden. Heute in fast jedem Kreditinstitut ins Datennetz integriert sind die Anwendungen Zutrittskontrolle, Alarmübertragung und Videotechnik. Die Zutrittskontrollsysteme der einzelnen Filialen oder Verwaltungsgebäude können von zentraler Stelle administriert werden. Zutrittsberechtigungen für einzelne Personen können je Filiale angelegt und gelöscht werden. Dies erleichtert einen flexiblen Personaleinsatz erheblich.

Die Alarmaufschaltung in Standleitungsqualität (Anforderung der Versicherer) erfolgt über das Datennetz der Bank. So können die Alarmierungswege im kundeneigenen Datennetz mehrfach redundant zusammengefasst und dann über, je nach Konzept, eine oder mehrere private Standleitungen zur entsprechenden hilfeleistenden Stelle weitergeleitet werden. Dabei ist es durchaus üblich, je nach Art der Meldung unterschiedliche Empfangsziele zu definieren. Überfallalarms können direkt auf die Polizei aufgeschaltet werden, Brandalarms direkt zur Feuerwehr und Einbruchmeldealarms beispielsweise auf eine private Leitstelle. Die Anbindung der hilfeleistenden Stellen wird über entsprechende Firewalls gegen unbefugte Zugriffe gesperrt. Auf diese Weise lassen sich in Datennetzen optimale Alarmierungs- und Überwachungssysteme sehr kostengünstig betreiben.

Die in den Filialen vorhandenen Videosysteme speichern Bilder im Normalfall lokal. Nur im Alarmfall können Bilder über das Datennetz übertragen werden. So lassen sich wichtige Beweisbilder sehr zeitnah zu Fahndungszwe-



Mehr über den Einsatz sicherungstechnischer Komponenten in bestehenden Netzwerken referiert der Autor auf den vom Bundesverband der Hersteller- und Errichterfirmen von Sicherheitssystemen e.V. (BHE) veranstalteten „Essener Sicherheitstagen“, 13./14.11. (Infos unter www.bhe.de).

cken bereitstellen oder sogar das Geschehen in einer Filiale während eines Überfalls live beobachten. Die vorgeschriebenen Funktionskontrollen lassen sich großteils von zentraler Stelle durchführen, ohne dass hierdurch zusätzliche Kosten für Wählleitungen entstehen. Auf den Einsatz zusätzlicher Maßnahmen zur Datensicherheit (Verschlüsselung) kann aufgrund der geschlossenen Benutzergruppe und den hohen Sicherheitsbestimmungen in Banknetzen meist verzichtet werden.

Anwendungsbeispiel „Industriebetrieb mit mehreren Gebäuden und einem Zweigwerk“:

Ein Industriebetrieb mit mehreren Gebäuden am Hauptsitz und einem Zweigwerk besitzt ein Zutrittskontrollsystem, CCTV-Systeme und mehrere Brand- und Einbruchmeldeanlagen. Alle Systeme sind über das vorhandene TCP/IP-Datennetz auf einen zentralen Sicherheitsleitstand aufgeschaltet. Die netzwerkfähigen Zutrittskontrollierer in den verschiedenen Bereichen des Unternehmens sind an das Netz angebunden. Das System lässt sich somit zentral vom Sicherheitsleitstand administrieren.

Durch die Vernetzung der vorhandenen Einbruchmelde- und Brandmeldeanlagen (EMA/BMA) können die Meldungen am lokalen Leitstand übersichtlich visualisiert werden.

In besonders sicherheitsrelevanten Bereichen im Betriebsgelände sind netzwerkfähige CCTV-Systeme installiert. Betriebsabläufe lassen sich überwachen und die schnelle Verifikation von Meldungen der EMA/BMA wird ermöglicht.

Bei Nicht-Besetzung des lokalen Leitstandes, werden sämtliche Alarmerungs- und Überwachungsfunktionen zu einem externen Dienstleister aufgeschaltet. Diese Anbindung erfolgt über eine dauerüberwachte TCP/IP-Standleitung für alle Anwendungen. Diese Anbindung ist durch die Verwendung von Firewalls gegen unberechtigte Zugriffe geschützt. Für die Alarmweiterleitung werden spezielle Komponenten, inklusive verschlüsselter Übertragung und besonderen Überwachungsmaßnahmen, eingesetzt um den höchsten Anforderungen an Übertragungssysteme zu genügen.

*Dipl.-Ing. Stephan Holzem ist tätig im Produktmanagement der TAS Telefonbau A. Schwabe GmbH & Co. KG, Mönchengladbach, und Mitglied im Fachausschuss Übertragungs- und Netzwerktechnik des BHE.
Kontakt zum Autor per E-Mail: sholzem@TAS.de*

Anzeige

Woche für Woche exklusive News

Abonnenten des Sicherheits markt sind schneller informiert. Im neuen kostenlosen Newsletter erhalten Sie jede Woche News der Branche kompakt, per Fax oder E-Mail, und ausführlicher im Internet im passwortgeschützten Bereich unter www.sicherheits-markt.info.