Hinweise und Handreichungen zur Planung von sicheren Netzen und Übertragungsstrecken zum Anschluss von Leitstellen im BOS Digitalfunk

Veröffentlichung des AK BOS-Leitstellen
von BITKOM und PMeV

Version 1.1

BITKOM

PMeV
PROFESSIONELLER MOBILFUNK e.V.
... mit Sicherheit besser!

Impressum

Herausgeber:	BITKOM Bundesverband Informationswirtschaft, Telekommunikation und neue Medien e. V. Albrechtstraße 10 A 10117 Berlin-Mitte Tel.: 030.27576-0 Fax: 030.27576-400 bitkom@bitkom.org www.bitkom.org	Bundesverband Professioneller Mobilfunk e.V. (PMeV) c/o: RA Rainer Ihde Schönhauser Alle 10-11 10119 Berlin info@pmev.de www.pmev.de
Ansprechpartner:	Michael Barth Tel.: 030.27576-102 m.barth@bitkom.org	Uwe Jakob Tel.: 02841.3913254 jakob@pmev.de
Redaktion:	Sebastian Rottmann (GeNUA), Thomas Buch (Rohde & Schwarz)	
Gestaltung / Layout:	Design Bureau kokliko / Anna Müller-Rosenberger (BITKOM)	

Hinweise und Handreichungen zur Planung von sicheren Netzen und Übertragungsstrecken zum Anschluss von Leitstellen im BOS Digitalfunk

Veröffentlichung des AK BOS-Leitstellen
von BITKOM und PMeV

Version 1.1

BITKOM

PMeV
PROFESSIONELLER MOBILFUNK e.V.

Inhaltsverzeichnis

Vorwort

Die Einführung des bundeseinheitlichen BOS-Digitalfunks ist gerade aus Sicht der Leitstellen eine hochkomplexe Thematik. Nutzer, Planer und Hersteller müssen mit einer neuen Technik, aber auch grundlegend anderen Strukturen und Organisationen umgehen. Der bundeseinheitliche Funk bietet eine Vielzahl verbesserter und neuer Leistungsmerkmale, überrascht aber auch immer wieder durch unvorhergesehene Schwierigkeiten.

Der Aufbau des BOS-Digitalfunks schreitet voran und verlangt rasche Lösungen von allen Beteiligten. In dieser Situation entsteht notwendigerweise eine Vielzahl sehr verschiedener Ansätze mit individuellen Architekturen, Komponenten und Schnittstellen, die nur sehr selten untereinander kompatibel sind, erhebliche Folgekosten für alle Beteiligten sind daher absehbar.

Vor diesem Hintergrund haben sich die in den Industrieverbänden BITKOM und PMeV organisierten Hersteller von Leitstellen und Leitstellenprodukten im Sommer des Jahres 2010 in der Arbeitskreis (AK) BOS-Leitstellen zusammengefunden, mit dem Ziel, gemeinsame Grundlagen für die Anbindung der Leitstellen an den BOS-Digitalfunk zu formulieren. Diese Anstrengung wird unterstützt durch die Arbeitsgruppe Leitstellen, in der sich die Bedarfsträger der Länder zusammengefunden haben, ebenfalls um Information auszutauschen und ihr Vorgehen abzustimmen.

Die Ergebnisse der herstellerübergreifenden Arbeit des AK sollen über die Publikationswege der Verbände, über PMRExpo und AG Leitstellen allen interessierten Parteien zur Verfügung gestellt werden um in Planungen, Ausschreibungen und Produktentwicklungen einzufließen.

Folgende Vorteile will der AK BOS-Leitstellen erzielen:

- Planungssicherheit für die Bedarfsträger
- Ausschreibungssicherheit für Nutzer, Planer und Hersteller
- Kostenreduktion bei Nutzern, Planern und Herstellern
- Vermeidung von mehreren Produktlinien (Modifikationen), damit auch höherer Investschutz
- Regelmäßiger Dialog und Verifizierung der Ergebnisse mit BDBOS und BSI

In diesem Rahmen sind auch die vorliegenden „Hinweise und Handreichungen zur Planung von sicheren Netzen Übertragungsstrecken zum Anschluss von Leitstellen im BOS-Digitalfunk“ entstanden. Sie sollen Orientierung bieten und aufzeigen, welche Optionen für die Anbindung der Leitstellen über IP-Strecken zur Verfügung stehen.
In aller Regel sind ja im Bundesland bereits vorhandenen Netze zu nutzen, die spezifische Strukturen und Restriktionen aufweisen. Gleichzeitig ist den hohen Sicherheitsanforderungen von BDBOS und BSI zu genügen.

Die Handreichungen wurden durch Herrn Sebastian Rottmann (GeNUA) und Herrn Thomas Buch (Rohde & Schwarz) gemeinschaftlich für den AK BOS-Leitstellen in der Unterarbeitsgruppe Technik erarbeitet und mit den anderen interessierten Herstellern abgestimmt.

Im Auftrag des AK BOS-Leitstellen Gruppe Technik

Dr. Jürgen Machui
(accellonet GmbH)

1 Einleitung

Mit der Einführung des digitalen Behördenfunks kommen auch auf Leitstellen Veränderungen zu. Ein zentraler Aspekt sind neue Anschaltkonzepte und die Vernetzung von Leitstellen. Denn für die effiziente Koordinierung von Einsätzen benötigen Leitstellen Sprach- und Datenverbindungen untereinander. Dabei dürfen die relevanten Anforderungen und Vorschriften nicht außer Acht gelassen werden.

Diese Broschüre richtet sich an Hersteller und Planer, die sich mit Leitstellen und deren Vernetzung beschäftigen. Sie geht auf die BDBOS- bzw. BSI-konforme Vernetzung von Leitstellen ein und gibt Empfehlungen für die Auswahl der richtigen Technologie.

1.1 Leitstellen müssen sich vernetzen. Die sichere Vernetzung von Leitstellen

Über öffentliche Netze übertragene Daten sind genauso schlecht gegen Mitleser geschützt wie eine Postkarte in der gelben Briefpost. Da für eine übergreifende Arbeit und Kooperation der Behörden und Organisationen mit Sicherheitsaufgaben aber ständig auch eingestufte oder sensible Informationen übertragen werden müssen, ist eine leistungsfähige und zuverlässige Lösung für eine sichere Datenübermittlung erforderlich. Dabei sind die Netze so abzusichern, dass vertrauliche Daten keinesfalls unautorisierten Personen zur Kenntnis gelangen bzw. von ihnen verfälscht werden können. Denn die Übertragung der Daten und Sprache findet oft über öffentliche Netze statt. Aber auch in eigentlich abgeschlossenen Netzen, wie einem eigenen Polizeinetz, sollte die Leitstellenkommunikation noch zusätzlich abgesichert werden.

Die Absicherung erfolgt über so genannte virtuelle private Netze (VPN) unter Verwendung kryptographischer Sicherungsmechanismen. Dabei dienen Kryptosysteme zum Aufbau verschlüsselter Verbindungen und Netze, die den sicheren Transport der Daten von einer Leitstelle zur anderen gewährleisten.

Die Anbindung von abgesetzten Leitstellen wird in Abhängigkeit der beim Nutzer vorhandenen Infrastruktur und des zur Verfügung stehenden Übertragungsnetzes unterschiedlich erfolgen. Um die Absicherung der Kommunikation über „unsichere“ öffentliche Übertragungsnetze zu erreichen, werden an den Hausübergängen der Leitstelle zum Übertragungsnetz des Betreibers Kryptosysteme positioniert, die den abgehenden und den ankommenden Daten- und Sprachverkehr möglichst verlustfrei und flexibel ver- bzw. entschlüsseln.

1.2 VS-NfD Krypto als Standard

Die im Behördenbereich zur Datenverschlüsselung verwendeten kryptografischen Systeme unterliegen besonderen Anforderungen. Diese werden durch die Zulassung für IT-Systeme vom Bundesamt für Sicherheit in der Informationstechnik (BSI) gewährleistet. Auch bei der Vernetzung von Leitstellen ergeben sich Anforderungen an das Zulassungslevel.

Durch die Einstufung des Kernnetzes der BDBOS nach VS-NfD (VS-NUR FÜR DEN DIENSTGEBRAUCH) müssen auch landesinterne und kommunal strukturierte Leitstellennetze nach VS-NfD abgesichert werden. Denn eine Kette ist immer nur so stark wie ihr schwächstes Glied. Es muss daher ein einheitliches Grundschutzlevel für das gesamte Netz gelten.

Daher gilt für alle Leitstellennetze, egal ob Polizei, Feuerwehr oder Rettungsdienst: Wenn eine Vernetzung stattfindet, dann ist eine Verschlüsselung mit VS-NfD Kryptosystemen zwingend erforderlich, da der Anschluss an das Kernnetz der BDBOS ansonsten nicht gestattet wird.

Die BDBOS stellt hierzu fest, dass die von den Bedarfsträgern geplante abschnittsweise Verschlüsselung zwischen dem KVMS-Gateway und Leitstellenarbeitsplätzen nur mit vom BSI freigegebenen Komponenten und Verfahren

zulässig ist (Feststellung der BDBOS aus: PMeV & BITKOM Workshop vom 18.11.2010, Nr.35F).

Der Netzabschlusspunkt für den Betreiber des Kernnetzes endet am sogenannten „Sandwich“. An dessen Ende werden meistens Konzentratoren eingesetzt, um die Anbindung der Leitstellen hinsichtlich Kosten und Komplexität so gering wie möglich zu halten. Um die einzelnen Leitstellen an die Konzentratoren heranzuführen, müssen diese mit dem Konzentrator vernetzt werden. Hierfür stehen BSI-konforme Technologien auf Basis von Schicht 2 (Layer-2) und Schicht 3 (Layer-3) des OSI (Open Systems Interconnection)-Schichtenmodells zur Verfügung.

Die eingesetzte Verschlüsselung der beiden Technologien hat dabei keinen Einfluss (Laufzeiten, Sprachqualität, etc.) auf die Ende-zu-Ende-Verschlüsselung die die Endgeräte verwenden. Die zusätzliche Verschlüsselung ist notwendig, da neben der Sprache auch Datendienste ins Kernnetz transportiert werden. Ferner findet unter den Leitstellen selbst auch Kommunikation, wie beispielsweise eine Synchronisation von Leitstellen-Datenbanken, statt. Auch diese Kommunikationsbeziehungen sind für Angreifer interessant und müssen deshalb bestmöglich geschützt und folglich mit VS-NfD Verfahren verschlüsselt werden.

2 Technologien

Bei der Vernetzung von IT-Systemen stehen prinzipiell zwei verschiedene Lösungen zur Verfügung. Diese basieren auf unterschiedlichen Technologien. Eine basiert auf Schicht 2, die andere basiert auf Schicht 3 des ISO-/OSI-Schichtenmodells.

Für beide Technologien gibt es Produkte, die vom BSI nach VS-NfD zugelassen sind. Da sich beide Technologien in Ihren Grundlagen unterscheiden, werden diese im folgenden Abschnitt genauer erläutert. Somit kann schon in der Planungsphase eine passende Wahl getroffen, bzw. beide Technologien in Kombination eingesetzt werden.

2.1 Layer 2-Technologie

2.1.1 Was ist Layer-2 Krypto

Bei der verschlüsselten Kommunikation auf Schicht 2 des OSI-Modells (Layer 2) werden Informationen (z.B. Sprache, Daten, Video) bereits auf einer unteren physikalischen Ebene chiffriert.

Da die Verschlüsselung der Datenpakete bei Layer 2-Vernetzungen bereits auf der Sicherheitsschicht erfolgt, wird zusätzlicher Overhead für die Sicherheit vermieden. Damit wird eine gleichbleibend hohe Übertragungsleistung bei minimaler Verzögerung (Latenz) erreicht. Last- oder paketgrößenabhängige Performanceschwankungen werden vermieden und die zur Verfügung stehende Bandbreite der Übertragungsleitung optimal ausgenutzt. Zum Anschluss einer Außenstelle an ein Netzwerk müssen für die verschlüsselte Layer 2 Datenübertragung lediglich zwei Kryptosysteme transparent in eine bestehende Ethernet-Netzwerk-Infrastruktur eingebunden werden (Punkt-zu-Punkt-Verbindung). Auch für eine sternförmige Anbindung von mehreren Außenstellen an ein Ethernet-Übertragungsnetz mit zentralem Knoten (z.B. Konzentrator-Standort), stehen VS-NfD zugelassene Kryptosysteme zur Verfügung (Punkt-zu-Mehrpunkt-Verbindungen).

2.1.2 Vorteile von Layer 2-Technologien

Die Beachtung der Forderung nach einer Sicherung der Informationsübertragung zwischen zu den Leitstellenstandorten auf dem Niveau VS-NfD führt aus dem Aspekt der Optimierung der Betriebskosten zu der Suche nach einer maximalen Ausnutzung der vom Provider oder Übertragungsnetz-Betreiber zur Verfügung gestellten Nutzdatenrate. Die Nutzung von Ethernet-Technologien (ISO OSI Layer 2) ermöglicht hierbei eine Minimierung des durch die Verschlüsselung der Daten notwendigen Sicherheits-Overheads und in der Folge eine Optimierung der Betriebskosten.

Mit der alternativen Verwendung von Ethernet-Diensten zur Leitstellen-Anbindung lassen sich gegenüber einer Anbindung mittels IP-Übertragungsdiensten oder SDH-basierter Standort-Anbindung folgende Vorteile erzielen:

- Optimale Ausnutzung der Übertragungskapazitäten (Nutzdatenrate) und damit
- Reduzierung der monatlichen Betriebskosten über die Laufzeit (OPEX)
- Reduktion der monatlichen Betriebskosten durch weniger Pflegeaufwand der IT-Sicherheitsbeziehungen
- Deutlich reduziertes Angriffspotential durch Grundsicherung der Kommunikationsbeziehungen zwischen den Standorten auf ISO OSI Layer 2

Die Layer 2 Kryptosysteme lassen sich transparent in die bestehende Ethernet-Netzwerkinfrastruktur zwischen den Standorten einbinden, so dass umfangreiche Konfigurationsänderungen ausbleiben können. Nach dem Rollout der Geräte fallen kaum Wartungsarbeiten an, so dass sich die Betriebskosten auf ein Minimum beschränken. Die Synchronisierung der Gegenstellen erfolgt automatisch, genau wie der periodische Wechsel der kryptografischen Schlüssel (Session Keys).

Die verzögerungsfreie Übertragung von Datenpaketen auf der Sicherungsschicht in Ethernet-Netzwerken ist eine

interessante Alternative zu konfigurationsaufwändiger und meist langsamerer Verschlüsselung auf höheren Schichten des OSI-Modells (z.B. IPSec in Layer 3-Netzen). Layer 2-Verschlüsselung ermöglicht Datendurchsätze in Gigabit-Geschwindigkeit und nutzt die verfügbare Bandbreite optimal aus.

2.1.3 Was muss man beachten

Viele Carrier oder Anbieter von Übertragungsdiensten zwischen verzweigten Leitstellen-Standorten bieten heute neben den bekannten Anschlusstechnologien wie Layer 3 (IP/IPSec), Standleitungen, SDH oder Frame Relay auch flächendeckende Ethernet-Services (Layer 2) an. Diese Ethernet-Dienste werden als EPL-, EVPL- oder ELAN-Services vom Service-Provider zur Verfügung gestellt. Zum Betrieb von Punkt-zu-Mehrpunkt-Verbindungen zwischen den Standorten werden VLAN-fähige Ethernet-Verbindungen benötigt, die ebenfalls von verschiedenen Anbietern als gesicherte VPN-Dienste auf Layer 2 Ethernet-Basis zur Verfügung gestellt werden.

Je nach Anforderung des Nutzers werden die Ethernet-Verschlüsselungssysteme vom Service-Provider als Verschlüsselungs-Dienst zur Verfügung gestellt und administriert, oder vom Nutzer selbst in die vorhandenen Verbindungen des Übertragungsnetzes zwischen Service-Provider und Leitstellenstandort eingebracht und administriert.

2.1.4 Installation, Konfiguration, Rollout und Betrieb

Beim Einsatz von Ethernet-Verschlüsselungsgeräten bleiben vorhandene IP-Adressbeziehungen zwischen Leitstelle und Konzentrator weiter bestehen, da die Daten auf höheren Transportebenen (ISO OSI Layer 3-7) nach der Entschlüsselung am Endpunkt der Übertragung unverändert wieder zur Verfügung stehen. Diese Eigenschaft der Layer 2- Ethernet-Technologie auf den unteren Transportebenen vereinfacht die Installation und Konfiguration von Ethernet-Verschlüsselungsgeräten, da die Geräte als quasi „transparentes“ Netzelement in die bestehenden IP-Beziehungen zwischen Leitstelle und Konzentrator eingesetzt werden können. Voraussetzung ist, dass die Übertragungsstrecke des Providers als Ethernet-Dienst zwischen den Standorten und zum Konzentrator geschaltet ist.

2.1.4.1 Installation und Konfiguration

Der Aufbau und die Inbetriebnahme von verschlüsselten Leitstellen-Verbindungen mittels Ethernet-Übertragungsdiensten (Layer 2) kann abschnittsweise und nach Bedarf oder vor dem Beginn des Regelbetriebes erfolgen. Zuerst werden die vorhandenen aktiven Netzkomponenten zwischen der LAN- und WAN-Seite der abgesetzten Leitstelle und dem Konzentrator vorkonfiguriert und installiert. Danach kann das Redundanz- und Umschaltverhalten im Fehlerfalle vorbereitet und überprüft werden (Umschaltung auf die Backup-Leitung). Wenn diese Vorarbeiten erfolgreich abgeschlossen sind, besteht bereits ein funktionierender Daten- und Kommunikationsweg zwischen der Leitstelle und dem Konzentrator oder weiteren nachgeordneten Leitstellen. Im nächsten Schritt werden die Ethernet-Verschlüsselungsgeräte zunächst im „Plain-Mode“ in diese Kommunikationsleitung eingeschleift und die Verbindung zum Sicherheits-Managementsystem hergestellt. Die Sprach- und Datenkommunikation erfolgt nun testweise über die Ethernet-Verschlüsseler im unverschlüsselten Modus. Wenn auch diese Installations- und Konfigurationsphase erfolgreich abgeschlossen ist, erfolgt die finale Umschaltung auf den Regelbetrieb der Geräte im Modus „VS-NfD-Verschlüsselung“.

2.1.4.2 Rollout

An die Ethernet-Verschlüsselungsgeräte selbst werden keine besonderen Anforderungen zur Lagerung oder den Versand an die abgesetzte Leitstelle gestellt. Dieses ist besonders bei einer größeren Anzahl von gleichzeitigen Installationen (Rollout-Szenarien) oder bei der Vorhaltung von Ersatzgeräten wichtig. Die Ethernet-Verschlüsselungsgeräte werden erst in Verbindung mit einer separat gelieferten USB-Smartcard (Geräte-Token) und der Verbindung zum Sicherheits-Managementsystem „scharf

geschaltet“. Die Schlüsselaushandlung und die Schlüsselwechsel zwischen den Ethernet-Verschlüsselungsgeräten erfolgen danach vollkommen autark. Eine permanente Online-Kommunikation zwischen Sicherheitsmanagement-Server und Ethernet-Verschlüsselungsgeräten ist nicht erforderlich (Polling-Verfahren, im Fehlerfall Störungsmeldung an übergeordnete Systeme). Nach der Erstinstallation wird der Geräte-Token wieder vom Ethernet-Verschlüsselungsgerät entfernt und während des Regelbetriebes sicher am Leitstellen-Standort verwahrt. Bei einem Gerätedefekt erlernt ein beliebiges Ersatzgerät mithilfe des verwahrten Geräte-Tokens die komplette Konfiguration des fehlerhaften Gerätes vor Ort und kann die Aufgaben des defekten Geräte umgehend übernehmen.

2.1.4.3 Betrieb

Wichtig für einen reibungslosen Betrieb der Verschlüsselungsgeräte ist ein leicht bedienbares und rollenbasiertes Sicherheits-Managementsystem. Durch die Trennung von Aufgabenbereichen wie z.B. Manager, Administrator und Beobachter, lassen sich abgestufte Operating-Konzepte und die sicherheitstechnische Trennung der „Geheimnisse“ durch die personelle Aufgabentrennung realisieren.

Diese meist nach dem Client-Server-Konzept aufgebauten Managementsysteme der Verschlüsselungsgeräte bestehen aus einem oder mehreren aufgebauten Sicherheitsservern (Ausfallredundanz) und abgesetzten Software-Clients, die den Zugriff und die Geräteadministration durch die Sicherheitsmanager über geschützte Internetverbindungen von jedem Standort aus ermöglichen.

Bei Bedarf werden auch Operating-Konzepte unterstützt, die Betreibern/Providern einerseits die Administration der Netzwerkfunktionalität der Geräte (meist über das SNMP-Protokoll) und andererseits den Bedarfsträgern/Nutzern das eigentliche Schlüsselmanagement als separate Funktionalität ermöglichen. Dies wird durch eine physikalische Trennung der Bereiche innerhalb der Ethernet-Verschlüsselungsgeräte (separate Schnittstellen) sowie durch getrennt ausgeführte Softwareinstanzen im Sicherheits-Managementsystem erreicht.

2.2 Layer-3-Technologien

2.2.1 Was ist Layer-3 Krypto

Das bekannteste Protokoll auf Layer-3 im OSI-Schichtenmodell ist IP (Internet Protocol). IP ist vor allem bekannt durch das heutzutage fast allgegenwärtige Internet bzw. die IP-Adresse. Kommunikation über IP-Netze ist per Voreinstellung ungesichert, das heißt es findet keine Verschlüsselung der Daten und auch keine Gewährleistung der Authentizität und Integrität statt. Diese Schutzziele werden bei IP mit dem zusätzlichen Verfahren IPsec erreicht. IPsec baut dabei sogenannte VPNs (virtuelle private Netzwerke) auf.

2.2.2 Vorteile von Layer 3 Technologien

Daraus ergeben sich mehrere Vorteile. IP ist zum Beispiel unabhängig vom Übertragungsmedium. Es ist somit egal, ob man ein Ethernet-, Mobil,- Funk- oder UMTS-Netz nutzt. IP findet über das so genannte Routing der IP-Pakete den Weg zum Zielsystem und IPsec sorgt dafür, dass die Kommunikation Ende-zu-Ende verschlüsselt ist und Fremde keinen Zugriff erlangen.

IP-Netze sind nahezu überall und von allen Providern verfügbar. IP-Netze können auch über die Grenzen eines einzelnen Providers aufgebaut werden. Sie bieten wie das Internet eine maximale Flexibilität für Anwender und deren Applikationen. Auch eine Anbindung von mobilen Lösungen (z.B. in Einsatzfahrzeugen oder in Form von Laptops) ist mit der IP-Technologie jederzeit möglich.

Ein weiterer Vorteil von Layer-3 basierten Netzen ist, dass Vollvermaschung erreicht werden. So können Leitstellen an Konzentratoren angebunden und jede Leitstelle mit jeder anderen, mit den gleichen Systemen, vernetzt werden, wie im Internet jeder Rechner auf jeden anderen zugreifen kann. Durch IP ist jedes Zielsystem adressierbar und erreichbar. Sollte eine Leitung ausfallen, finden die IP-Pakete einen alternativen Pfad und können die Daten weiterhin zustellen. Dabei muss man jedoch darauf achten,

dass innerhalb des Kryptosystems dynamische Routingfunktionen verfügbar sind. Hier wird auf das Routing mittels OSPF (Open Shortest Path First) verwiesen. Auch andere Vernetzungskonzepte wie Punkt-zu-Mehrpunktverbindungen (beim klassischen Anschluss mehrerer Leitstellen an einen Konzentrator) und Kombinationen mehrerer Konzepte sind auf Basis von Layer 3 möglich.

In Layer-3 Netzen ist QoS (Quality of Service) nutzbar. Damit kann bestimmten Applikationen (z. B. Sprache) Vorfahrt vor anderen Applikationen (z. B. E-Mail) gewährt werden. Informationen aus den OSI-Layern unterhalb der Schicht 3 bleiben dabei natürlich erhalten. Mit Layer-3 Kryptosystemen lassen sich beispielsweise auch VLANs übertragen und auswerten.

2.2.3 Was muss man beachten

Da VPNs (auf Layer 2 und 3) eine vollständige Kopplung zwischen Netzen darstellen, muss man auf den Einsatz von Firewalls achten. Viele Kommunikationsbeziehungen sind nur intern nötig und müssen nicht über ein gemeinsames Netz transportiert werden. Beispiele hierfür sind die heute weit verbreitete Verwundbarkeit von Desktop- und Serversystemen. Auch bei vermeintlich isolierten Netzen, wie bei Leitstellen, sind diese Gefahren nicht zu unterschätzen. Firewalls können beispielsweise bei einem Ausbruch eines Wurms dafür sorgen, dass infizierte Bereiche vom restlichen Netz isoliert werden. Somit hat man Zeit, sich um den Schädling zu kümmern. In Netzen ohne Firewalls verbreiten sich Schadprogramme meist sehr schnell und können schnell den kompletten Leitstellenbetrieb stillegen.Bei Firewalls muss man jedoch beachten, dass sich Paketlaufzeiten (Latenzen) erhöhen. Eine kleine Erhöhung der Latenz findet immer statt, wenn ein Layer-3 System wie zum Beispiel eine Firewall oder ein Layer-3 Kryptosystem durchlaufen wird. Diesen Durchlauf nennt man „Hop“. Obwohl dies nur wenige Millisekunden pro Gerät ausmacht, sollte man darauf achten, dass ein Kryptosystem auf Basis von Layer-3 eine Firewall beinhaltet und diese nicht durch ein zusätzliches System gestellt werden muss. Denn die Latenz steigt weniger an, wenn ein Gerät beide Funktionen übernimmt. Firewallsysteme unterliegen keiner Vorschrift zur Zulassung durch das BSI. Da bei Firewalls aber auch auf Qualitätssiegel geachtet werden muss, ist eine Zertifizierung nach Common Criteria wichtig. Hier ist auf eine Zertifizierung, mindestens in der Stufe EAL 4+, zu achten. Ein besonders wichtiger Punkt bei Firewallzertifizierungen ist der Baustein AVA. VAN. Dieser „Selbstschutz“ sollte in der Stufe 4 oder höher geprüft worden sein.

Es ist darüber hinaus zu beachten, dass bei der Verschlüsselung der Pakete ein entsprechender Overhead erzeugt wird. Vor das eigentliche IP-Paket wird der IPsec-Anteil angefügt. Das wirkt sich vor allem bei kleinen Paketen aus. Denn dort ist der IPsec-Anteil gegenüber dem Datenanteil entsprechend groß. Damit hier die Performance nicht einbricht, muss man sich bei der Evaluierung für ausreichend performante Systeme entscheiden und sich mit den Herstellern solcher Systeme abstimmen, welche Lösung zum geplanten Datenprofil passt. Dadurch ergibt sich aber auch der Vorteil, dass man meistens genau das für das eigene Netz geeignete System findet und Kosten für überdimensionierte Systeme einspart.

Ein weiterer Punkt ist der bevorstehende Umbruch bei IP-Netzen: Man geht davon aus, dass IPv6 (IP in der Version 6) das bisherige IPv4 (Version 4) bald verdrängen wird, da es kaum noch IPv4-Adressen gibt (Stand Januar 2011). Daher ist zu beachten, dass ein Layer-3 Kryptosystem schon heute mit IPv6 umgehen kann.

2.2.4 Installation, Konfiguration und Betrieb

2.2.4.1 Installation und Konfiguration

Installation und Konfiguration sollte mit zentralen Managementsystemen erfolgen. Gerade größere VPNs benötigen die Gesamtsicht auf das Netz. Ansonsten muss jedes System einzeln mit seinen Partner bekannt gemacht werden. Für Ausnahmefälle sollte eine lokale Oberfläche aktivierbar sein. Das Einlesen von Informationen wie MAC-Adressen oder Lizenzen sollte im Bulk-Verfahren möglich sein. Das heißt, dass dieser Schritt für

alle Systeme auf einmal erfolgt und nicht einzeln. Auch andere Aktionen ersparen viel Zeit, sofern sie sich über den Bulk-Modus ausführen lassen.

Da es sich bei Layer-3-Kryptierern um aktive Netzkomponenten handelt, muss die Konfiguration der IP-Adressen zuvor entsprechend geplant werden. Manche Systeme bieten die Möglichkeit LAN-seitig im Layer-2 Modus zu operieren. Wenn das Netzdesign so etwas zulässt, kann man Systeme sehr einfach im laufenden Betrieb einführen, ohne große Änderungen am lokalen Netzwerk zu planen.

Managementoberflächen sollten auf Basis einer Web-GUI arbeiten. Somit muss keine spezifische Software installiert werden. Möglicherweise kommt es andernfalls zu Problemen, da die Managementsoftware für das beim Kunden im Einsatz befindliche Betriebssystem oder deren Version nicht zur Verfügung steht. Web-GUIs hingegen laufen über Web-Browser, die normalerweise immer zur Verfügung stehen.

2.2.4.2 Rollout

Der Rollout von vielen Systemen sollte über Funktionen wie Templates erfolgen können. Damit kann man Systeme mit Basisfunktionen, wie einem Default-Gateway und einem Basis-Firewallregelsatz, ausstatten. Sobald die Systeme an ihren physikalischen Bestimmungsort stehen, bauen diese von sich aus eine Verbindung zum Managementsystem auf, holen sich von dort eine für sie abgestimmte Konfiguration ab, und laden diese. Eine Funktion mit der Rollouts über USB-Sticks möglich sind, kann in manchen Fällen hilfreich sein.

2.2.4.3 Betrieb

Aus betrieblicher Sicht sind folgende Punkte auf jeden Fall zu empfehlen: Einzelne Systeme müssen sich zu hochverfügbaren Clustern kombinieren lassen. Nur so kann man sich gegen den Ausfall eines einzelnen Systems absichern. Hierbei sollte man darauf achten, dass kurze Umschaltzeiten möglich sind. Hier darf die Verbindung nach einer HA-Übernahme nur wenige Augenblicke ausfallen. Hier muss aber das Gesamtkonzept des Netzwerkes beachtet werden, da verschlüsselte Verbindungen meist mehr Komponenten als nur die Kryptosysteme betreffen. Auch eingesetzte Managementsysteme müssen einen HA-Betrieb sicherstellen.

Beim Management von Layer-3 Kryptierern ist es wichtig, dass das IPsec-Schlüsselmaterial, das meist auf Chipkarten ausgelagert ist, erneuert werden kann, ohne dass man die Chipkarte dafür austauschen muss. Wenn sich Daten am Kryptosystem ändern, sollte keine Neuinitialisierung der Chipkarte nötig sein. Nach der ersten Chipkarteninitalisierung sollte sich alles „online“ erledigen lassen.

Ferner sind Systeme im Feld über ein zentrales Managementsystem einfach mit neuen Konfigurationen und Updates bespielbar. Für den Notfall sind solche Funktionen auch „offline“ über einen USB-Stick praktisch.

Das Managementsystem sollte ein abgestuftes Rollen- bzw. Rechtekonzept und die Mandantenfähigkeit für die Administration enthalten. Damit kann der Betrieb leichter durch eigenes Personal oder durch einen externen Dienstleister durchgeführt werden. Der Kanal zwischen Managementsystem und Kryptosystemen muss über sichere Verbindungen möglich sein. Hier bietet sich das Protokoll SSH an, da es maximale Flexibilität bei gleichzeitiger Sicherheit bietet. Kryptosysteme sollten aus Sicherheitsgründen nicht per SNMP konfiguriert werden bzw. nur, wenn ein separater kryptierter Kanal zur Verfügung steht. Lediglich das Auslesen von Informationen der Systeme per SNMP ist aus Sicherheitssicht unbedenklich.

Für den laufenden Betrieb ist es weiterhin wichtig, dass man sich lokal auf den Kryptosystemen einloggen kann und dort Tools zum Debugging hat. Hier sind klassische Tools wie netstat, tcpdump, ping oder traceroute zu nennen. Idealerweise lässt sich eine Verbindung auf die Konsole auch über das Managementsystem herstellen. Auch hier bietet sich SSH für Remote-Logins an.

3 Zusammenfassung

Betreiber von Leitstellen können heute, in Abhängigkeit von der jeweiligen regionalen Ausbaustufe des Provider-Netzes, Layer 2- oder Layer 3-Übertragungs-technologien, -Dienste, -Verfügbarkeiten und -Bandbreiten zum Anschluss Ihrer Leitstellen weitgehend frei wählen. Die jeweiligen Netzbetreiber vor Ort bieten meist flächen-deckend die entsprechenden Ethernet-, SDH-, oder IP-Übertragungsleitungen und –dienste an. Basierend auf der vorhandenen oder geplanten Netzinfrastruktur des Nutzers kann die wirtschaftlichste (Betrachtung über die gesamte Nutzungsdauer) und technologisch optimale Anschlusstechnologie ausgewählt werden.

Die Sicherheitsverantwortlichen für den BOS Digitalfunk erwarten für die Verarbeitung und Übertragung der Sprach- und Dateninformationen der BOS Leitstellen den Einsatz von entsprechend zugelassenen Verschlüsselungs-geräten mit einem Geheimhaltungsgrad von VS-NfD.

Erst die Kombination aus geplanter oder vorhandener Übertragungstechnologie und BSI-zugelassenen Ver-schlüsselungsgeräten auf Layer 2- oder Layer 3-Basis, ermöglicht beim Anschluss von BOS Leitstellen die optimale Auslastung des Übertragungsnetzes auf hohem geforderten Sicherheitsniveau (VS-NfD), ausreichender Verfügbarkeit sowie guter Sprach- / Datenqualität.

Die Auswahl der jeweiligen Verschlüsselungstechnik (Layer 2 oder Layer 3) erfolgt auf Nutzerseite nach wirt-schaftlichen oder technologischen Auswahlkriterien. Da die Verschlüsselungskomponenten direkt im Nutzdaten-weg eingesetzt werden und die Datenprofile beeinflussen können, sollten sie bereits frühzeitig bei der Planung entsprechender Leitstellenstandorte berücksichtigt wer-den. Manchmal ist auch eine Mischlösung zielführend, bei der Layer 2 und Layer 3-Technologien in geeigneter Weise miteinander kombiniert werden können.

Beide Technologien haben somit Ihre Vor- und Nach-teile. Für welche man sich entscheidet, hängt von vielen Rahmenbedingungen ab. Wichtig aber bleibt: Die im BOS Digitalfunk für die Kommunikation der Leitstellen einge-setzte Lösung muss vom BSI nach VS-NfD zugelassen sein.

Informationen zu Herstellern zugelassener Systeme sind über das BSI erhältlich:
Bundesamt für Sicherheit in der Informationstechnik
Referat 323 – Zulassungen und Prüfstandards
Telefon: 0228 99 9582 5525
49 (0) 3018 9582 5525
E-Mail: zulassung@bsi.bund.de

Der Bundesverband Informationswirtschaft, Telekommunikation und neue Medien e.V. vertritt mehr als 1.350 Unternehmen, davon über 1.000 Direktmitglieder mit etwa 135 Milliarden Euro Umsatz und 700.000 Beschäftigten. Hierzu zählen Anbieter von Software & IT-Services, Telekommunikations- und Internetdiensten, Hersteller von Hardware und Consumer Electronics sowie Unternehmen der digitalen Medien. Der BITKOM setzt sich insbesondere für eine Modernisierung des Bildungssystems, eine innovative Wirtschaftspolitik und eine zukunftsorientierte Netzpolitik ein.

Der Bundesverband Professioneller Mobilfunk e.V. (PMeV) ist ein Zusammenschluss führender Anbieter und Anwender von Kommunikationssystemen für den mobilen professionellen Einsatz. Seine Mitglieder sind Hersteller, System- und Applikationshäuser sowie Netzbetreiber und Nutzer. Ziel des PMeV ist es, den PMR-Markt in Deutschland weiter zu entwickeln. Als führender Kompetenzträger in Sachen PMR in Deutschland bietet er zu diesem Zweck ein Forum für einen neutralen, herstellerunabhängigen und partnerschaftlichen Dialog mit den Marktpartnern, der Politik sowie den Behörden und Institutionen.

BITKOM

Bundesverband Informationswirtschaft,
Telekommunikation und neue Medien e.V.

Albrechtstraße 10 A
10117 Berlin-Mitte
Tel.: 030.27576-0
Fax: 030.27576-400
bitkom@bitkom.org
www.bitkom.org

PMeV
PROFESSIONELLER MOBILFUNK e.V.

Bundesverband Professioneller
Mobilfunk e.V.

Kornstraße 35
47443 Moers
Tel.: 02841.3913254
Fax: 02841. 913255
jakob@pmev.de
www.pmev.de