Der Diözesandatenschutzbeauftragte

der Erzbistümer Berlin und Hamburg
der Bistümer Hildesheim, Magdeburg, Osnabrück und
des Bischöflich Münsterschen Offizialats in Vechta i.O.

DATENSCHUTZ
IN DER KATHOLISCHEN KIRCHE

Kurzbericht: Sicherheit bei der Voice over IP Telefonie (VoIP)

1. Hintergrund

Die Umstellung der analogen und ISDN-Telefonanschlüsse auf IP-Technologie (IP-Telefonie oder auch Voice over IP, VoIP) wird derzeit vorangetrieben. Beispielsweise hat die Telekom angekündigt, bis zum Jahr 2018 die von ihr betriebenen Festnetzanschlüsse u. a. aus Gründen der Technologie-Vereinheitlichung und damit einhergehender Kostenersparnis auf die in den Datennetzen genutzte und etablierte IP-basierte Technologie umzustellen. Das analoge sowie das digitale ISDN-Festnetz werden außer Betrieb genommen werden und die Sprach-Kommunikation erfolgt damit auf demselben Weg und auf Grundlage derselben Technologie wie beispielsweise die Nutzung des Internet. [1]

Betrachtet werden im Folgenden die beiden Fälle, in denen Provider-seitig ein analoger oder ISDN-Anschluss in einen VoIP-Anschluss umgewandelt wird, und:

1. Der Anschlussinhaber nichts an seiner Telefonanlage ändert und weiterhin mit analogen oder ISDN-fähigen Geräten telefonieren möchte („VoIP extern“).
2. Zusätzlich der Anschlussinhaber seine Telefonanlage auf VoIP fähige Komponenten umstellt und somit mindestens die analogen/ISDN-fähigen Telefone gegen IP-Telefone austauscht („VoIP intern“).

Beschränkt sich die VoIP-Technologie im ersten Fall auf das Netz des VoiP-Providers und endet am entsprechenden Router, wird diese im zweiten Fall auch im Netzwerk des Anschlussinhabers eingesetzt. Bei einer Umstellung erfolgt in beiden Fällen üblicherweise ein Austausch des seitens des Providers zur Verfügung gestellten Routers. In Fall 1 (VoIP extern) ist dann sicherzustellen, dass weiterhin ein Anschluss von analogen oder ISDN-Telefonen möglich ist.

In diesem Kurzbericht werden im zweiten Kapitel die besonderen Anforderungen im kirchlichen Umfeld beschrieben und im dritten Kapitel die Unterschiede zwischen analoger/ISDN-Telefonie und VoIP vorgestellt. Im vierten Kapitel werden die zusätzlichen Gefährdungen für die Informationssicherheit aufgezeigt, die mit diesem Technologiewechsel einhergehen, bevor im letzten Kapitel Sicherheitsmaßnahmen vorgeschlagen werden.

2. Besondere Anforderungen im kirchlichen Umfeld

Die Kirche bietet mit dem Betrieb von Beratungs- und Seelsorgestellen einige Leistungen an, bei denen die übermittelten Informationen zwischen kirchlichen Stellen und Externen unter die Schweigepflicht gemäß § 203 StGB fallen können.

Das Telefonat mit kirchlichen Beratungsstellen wie etwa der Telefonseelsorge ist üblicherweise gebührenfrei und sollte somit nicht im Einzelverbindungsnachweis der Telefonrechnung aufgeführt werden; so ist bei zentral verwalteten Anschlüssen, wie etwa in Unternehmen, anhand der Telefonrechnung dem Anschlussinhaber nicht ersichtlich, dass über seinen Anschluss ein solches gebührenfreies Telefonat geführt worden ist. Je nach Konfiguration der Telefone oder der Telefonanlagen auf Seiten der Gesprächspartner kann dabei allerdings nicht ausgeschlossen werden, dass Gesprächsdaten an anderer Stelle protokolliert und damit ggf. nachvollzogen werden können. Den Mitarbeitern dieser Stellen werden keine Rufnummern angezeigt, sodass die Anonymität des Anrufenden sichergestellt ist. Besondere Maßnahmen zur Sicherung der Vertraulichkeit der Gespräche, d.h. dedizierte Maßnahmen gegen das Abhören der Leitungen durch Unberechtigte, werden nicht ergriffen.

3. Unterschiede zwischen VoIP und herkömmlicher Telefonie

VoIP unterscheidet sich von der herkömmlichen Telefonie insbesondere bezüglich folgender Aspekte [2]:

1. Zuordnung der Teilnehmer: Im herkömmlichen Telefonnetz ist jeder Teilnehmeranschluss physisch über einen definierten Port mit einem Anschluss in der zugehörigen Vermittlungsstelle verbunden. Bei VoIP ist die Nutzung eines Teilnehmeranschlusses im Prinzip hingegen aus einem beliebigen Netz und von einer beliebigen IP-Adresse aus möglich.
2. Signalisierung und Vermittlung der Sprachdaten: Bei ISDN erfolgen die Signalisierung sowie die Übertragung der Sprachdaten über zwei verschiedene Kanäle (out-band), wobei der Kanal für die Sprachübertragung für die Zeit des Telefonats festgelegt ist (verbindungsorientierte Vermittlung). Bei VoiP hingegen erfolgen Signalisierung und Übermittlung der Sprachdaten innerhalb desselben Netzes (in-band). Die Sprachdaten werden in einzelnen Paketen übermittelt, wobei die für die Übermittlung genutzten Routen nicht identisch sein müssen (paketorientierte Vermittlung).
3. Endgeräte: Die meisten herkömmlichen Telefone sind auf die eigentliche Telefonfunktion beschränkt. Soll VoIP auch im internen Netz genutzt werden, können einerseits Softphones, d. h. auf PCs laufende Programme zur IP-Telefonie, andererseits eigenständige IP-Telefone verwendet werden. Letztere verfügen im Gegensatz zu den Softphones über eine eigene Netzschnittstelle und sind üblicherweise nicht mit Standard-PC-, sondern proprietären Betriebssystemen ausgestattet.

4. Zusätzliche Gefährdungen für VoIP

Die Gefährdungen der klassischen Telefonie bestehen für VoIP weitestgehend fort. Hinzu kommen Bedrohungen auf das Datennetz, über das die VoIP-Daten, bestehend aus Signalisierungs- sowie die Sprachdaten, gesendet werden, sowie netzwerkbasierte Angriffe auf die eingesetzten Geräte.

4.1 Verlust der Vertraulichkeit

In der Standardeinstellung der für die IP-Telefonie häufig verwendeten Protokolle SIP (Session Initiation Protocol, Übermittlung der Signaldaten) und RTP (Real-Time

Transport Protocol, Übermittlung der Sprachdaten) sind keine Maßnahmen zur Sicherstellung der Vertraulichkeit und Integrität enthalten, sodass diese Daten an allen Stellen, die sie passieren, abgehört werden können. Dies kann durch Missbrauch von Berechtigungen seitens der jeweiligen Administratoren oder durch einen Angriff geschehen, bei dem bestehende Schwachstellen in den beteiligten Systemen oder Anwendungen ausgenutzt werden.

Für den Fall 1, VoIP extern, betreffen diese zusätzlichen Gefährdungen lediglich das Provider-Netzwerk und die darin befindlichen Systeme bis einschließlich zum Router im Haus des Anschlussinhabers. Die Gefährdung des Abhörens durch Mitarbeiter des Providers innerhalb des von ihm administrierten Telefonnetzes besteht allerdings bereits für den Fall der herkömmlichen, d. h. analogen oder ISDN-Telefonie.

Im Fall VoIP intern, bei dem Sprach- und Signaldaten auch im Netzwerk des Anschlussinhabers kursieren, betrifft diese Gefährdung auch das Abhören durch die eigenen Administratoren oder das Ausnutzen von Schwachstellen in den selbst-betriebenen Systemen (einschließlich der Telefone) oder Anwendungen. Als Besonderheit bei den Endgeräten im VoIP Netz ist zu beachten, dass diese über eine IP-Adresse erreichbar sind und damit möglicherweise auch über das Internet erreicht und über Schwachstellen angegriffen werden können.

4.2 Verstoß gegen datenschutzrechtliche Bestimmungen

Die Management-Software für Telefon-Anlagen bietet oftmals umfangreiche und beispielsweise über ein Web-Interface leicht zugängliche Werkzeuge zur Erstellung und Auswertung von Telefonie-Daten. Hier gilt es darauf zu achten, dass die Nutzung möglicher Protokollier- und Auswertfunktionen datenschutzkonform erfolgt. Diese Funktionen werden unabhängig von der intern eingesetzten Telefontechnik angeboten, sind also im Fall 1 (VoIP extern) genauso einschlägig wie im Fall 2 (VoIP intern). Es besteht die Gefährdung, dass im Fall VoIP intern bei einer Umstellung von analoger/ISDN-Telefonie auf VoIP die Protokollierungsvorgaben nicht übernommen oder nicht korrekt übertragen werden können oder ggf. mögliche neue Funktionen wie die Raumschaltung falsch konfiguriert werden.

4.3 Verlust der Verfügbarkeit

Bei einem Ausfall des Datennetzes ist auch die VoIP-Telefonie, die über dieses Netz erfolgt, nicht mehr verfügbar. Dies kann durch technische Störungen innerhalb des Netzwerks ebenso wie durch einen Stromausfall erfolgen.

In beiden Fällen, VoIP extern und VoIP intern, hätte eine Störung des Providernetzes durch technische Störungen ebenso wie durch einen Stromausfall zur Folge, dass Telefongespräche nicht mehr geführt werden können. Im Fall 2, VoIP intern, können auch Netzwerkstörungen oder Stromausfälle auf Seiten des Anschlussinhabers, die den Router, die VoIP-Switche oder die Telefone betreffen, zum Verlust der Verfügbarkeit führen.

Des Weiteren kann eine Störung der Verfügbarkeit auch durch externe Angriffe auf zentrale Elemente des Providers (Fall 1) aber auch im Netz des Anschlussinhabers (Fall 2) erfolgen. Dazu zählt das Ausnutzen von Schwachstellen in Gateways oder durch das Erzeugen übermäßig vieler Anfragen (Denial of Service) an einzelne Komponenten.

4.4 Verlust der Integrität

An alle in Abschnitt 4.1 aufgeführten Stellen, an denen VoIP-Daten durch Missbrauch von Berechtigungen oder durch einen Angriff auf die Systeme abgehört werden können, können in der Standardeinstellung von SIP und RTP Sprachdaten auch verändert oder wiedereingespielt werden. Im Fall 1 betriff dies wiederum nur das Providernetz, im Fall 2 ebenfalls den Teil des Netzwerks des Anschlussinhabers, durch den VoIP-Daten fließen.

5. Maßnahmen zur Absicherung der IP-Telefonie

Für den Fall 1 (VoIP extern) betreffen die im Folgenden vorgestellten Sicherheitsmaßnahmen den Provider, im Fall 2 (VoIP intern) sind die aufgeführten Maßnahmen auch seitens des Anschlussinhabers zu berücksichtigen.

5.1 Grundlegende Sicherheitsmaßnahmen

Gemäß den Empfehlungen des BSI [2] und des NIST [3] sind alle Standard-Maßnahmen zur Absicherung von IP-Netzen sowie zur Absicherung von Clients und Servern (z. B. minimal konfigurierte und gehärtete Systeme, aktueller Patch-Stand) auch in VoIP-Umgebungen umzusetzen und auf die zusätzlichen Komponenten, wie z. B. die IP-Telefone auszuweiten.

5.2 Maßnahmen zur Zutritts- und Zugangskontrolle

Es sind Maßnahmen zur Zutrittskontrolle für den physischen Zugang ebenso wie zur Zugangskontrolle in einem entsprechenden Berechtigungskonzept umzusetzen. Administratoren und Nutzern müssen die entsprechenden Rollen und Berechtigungen nach dem Need-to-know-Prinzip zugewiesen werden. Es wird weiterhin empfohlen, administrative Zugänge zu sämtlichen VoIP-Komponenten über eine Zwei-Faktor-Authentisierung zu schützen, um einem unberechtigten Zugang vorzubeugen. Die Administration sollte idealerweise über verschlüsselte Protokolle erfolgen und die Möglichkeit der Remote-Konfiguration auf das Notwendige eingeschränkt werden; dazu zählen auch ggf. vorhandene Konfigurationsmöglichkeiten über Web-Interfaces.

Im Fall 2, VoIP intern, sollte grundsätzlich eine Trennung von Daten- und Sprachnetz, beispielsweise über VLANs eingerichtet werden. Auf diese sollte nur in Ausnahmefällen verzichtet werden.

5.3 Update- und Patch-Management

In beiden Fällen, VoIP extern sowie VoIP intern, ist der Router regelmäßig mit Updates zu versorgen und in die entsprechenden Patch- und Update-Prozesse mitaufzunehmen. Im Fall VoIP intern sind ferner alle durch den Einsatz von VoIP hinzugekommenen Systeme wie z. B. zusätzliche Server, Sicherheitsgateways und insbesondere die Endgeräte mit Updates zu versehen. Auf diesen können beispielsweise Konfigurationsdaten ausgelesen werden, mit denen Weiterleitungen eingerichtet und z. B. Abrechnungsbetrug begangen werden kann.

5.4 Maßnahmen zur Sicherstellung der Verfügbarkeit

In beiden Fällen VoIP extern sowie VoIP intern werden Telefongespräche ausschließlich über das Datennetz des Providers geführt, sodass bei dessen Ausfall auch die Telefoniefunktion nicht mehr zur Verfügung steht. Hier ist zu prüfen, welche Verfügbarkeitszeiten benötigt und seitens des Providers zugesichert werden.

Im Fall 2, VoIP intern, sollte durch Monitoring des Netzwerkverkehrs und eine entsprechenden Analyse Störungen der Verfügbarkeit im eigenen Netzwerk, die zu einer Beeinträchtigung der Verfügbarkeit führen können, vorgebeugt werden (s. auch Abschnitt 0). Bei Einsatz eines Sicherheitsgateways sollte auf dessen VoIP-Fähigkeit geachtet werden, die dafür sorgt, dass nicht unnötigerweise große Port-Bereiche dauerhaft von extern angesprochen werden können, sondern diese nur für die Übermittlung von VoIP-Daten geöffnet werden. Ferner gibt es besondere Anforderungen an eine hohe Durchsatzmöglichkeit im Hinblick auf zu verarbeitende Pakete. Die Gefahr eines Denial of Service-Angriffs ist bei VoIP hoch. Für diesen Fall ist sicherzustellen, dass die Systeme nach einem Ausfall möglichst bald wieder zur Verfügung stehen. Konfigurationseinstellungen der Geräte müssen daher bei der Erstellung von Datensicherungsplänen besondere Beachtung finden.

Im Fall VoIP extern und bei der weiteren Benutzung der vorhandenen ISDN-Telefone ist zu beachten, dass ISDN-Telefone üblicherweise über den NTBA mit Strom versorgt werden können, der bei VoIP nicht mehr vorhanden ist. Je nachdem wie die Stromversorgung erbracht wird, sollte für den Fall eines Stromausfalls einerseits der VoIP-Router ebenso wie zumindest die wichtigsten Telefone über eine Unterbrechungsfreie Stromversorgung (USV) mit Notstrom versorgt werden können.

Auch im Fall VoIP intern ist eine USV für alle zentralen VoIP Komponenten (Router, wichtige Endgeräte, etc.) einzurichten. Evtl. sollte ein Notbetrieb über Mobilfunkgeräte geplant werden.

Ebenso sind im Fall VoIP zentrale Komponenten redundant vorzuhalten, um bei einem Geräteausfall möglichst schnell den Normalbetrieb wiederaufnehmen zu können.

5.5 Verschlüsselung der Kommunikation

Werden Informationen mit hohem Schutzbedarf kommuniziert, sollte eine Verschlüsselung der Sprachdaten realisiert werden. Dies kann über die Verwendung von SRTP (Secure Real-Time Transport Protocol) zum Versand der Sprachdaten erreicht werden; allerdings ist hierfür ein geeignetes Schlüsselmanagement unter den beteiligten Kommunikationspartner einzurichten. Eine Alternative für die Verschlüsselung der Sprachdaten, das dieses Problem behebt bietet das Protokoll ZRTP (Z-Real-Time Transport Protocol). Bei Bedarf ist darauf zu achten, dass die eingesetzte Hard- und Software diese Protokolle unterstützt.

Zum Schutz der Signaldaten besteht die Möglichkeit der Übertragung der SIP-Pakete unter Verwendung des TLS-Protokolls, welches die einseitige oder gegenseitige Authentifizierung unterstützt.

5.6 Protokollierung

Im Hinblick auf die Protokollierung empfiehlt das BSI [4] eine systematische und verbindliche Protokollierung festgelegter Parameter und eine regelmäßige Auswertung dieser Informationen. Bei der Signalisierung wird beispielsweise eine Protokollierung der Kommunikationspartner, der -dauer, ob das Gespräch angenommen wurde, und von wo aus das Gespräch geführt wurde vorgeschlagen. Neben der Protokollierung von Kommunikationsinformationen wird empfohlen, auch die Systemzustände und Ereignisse auf der VoIP-Anlage zu protokollieren und auszuwerten, um beispielsweise Störungen oder unberechtigte Zugriffsversuche frühzeitig erkennen und angemessen gegensteuern zu können. Weitere Details sind der Maßnahme M 4.292 in [4] zu entnehmen.

6. Referenzen

[1] http://www.telekom.com/medien/medienmappen/Medienmappe+IP-Umstellung/260274, abgerufen am 14.01.2015

[2] Bundesamt für Sicherheit in der Informationstechnik, IP-Telefonie (Voice over IP), BSI-Leitlinie zur Internet-Sicherheit (ISi-L), 2008

[3] National Institute for Standards and Technology, Security Considerations for Voice Over IP Systems, Special Publication 800-58, 2005

[4] Bundesamt für Sicherheit in der Informationstechnik, IT-Grundschutz-Kataloge, 14. Ergänzungslieferung, 2014

Dr. Sascha Todt

Erstellt im Auftrag des Diözesandatenschutzbeauftragten
unter Mitwirkung der datenschutz nord GmbH