Security Journal GAI Netconsult GmbH April 2011

Datenschutz bei Einführung von Voice over IP

Bei der Einführung von Voice over IP nehmen die Konfigurationsmöglichkeiten gegenüber normalen TK-Anlagen sprunghaft zu. Ebenso nehmen jedoch auch die Gefahren für den Datenschutz der Mitarbeiter zu, die zu einer Rund-um-Überwachung führen können, die sich George Orwell in seinem Buch 1984 noch kaum vorstellen konnte.

Besonders bei der Einführung von CTI-Funktionen sind die Möglichkeiten des Administrators kaum durch die technischen Möglichkeiten beschränkt. Daher sollte der Betriebsrat jeder Firma darauf achten, nicht nur bei der Nutzung des Internets, sondern auch bei der Einführung neuer TK-Anlagen, CTI Software oder von Voice over IP darauf zu achten, dass die Kontroll- und Überwachungsfunktionen sowie die datenschutzrelevanten Leistungsmerkmale in beiderseitigem Einvernehmen von Unternehmen und Betriebsrat geregelt werden. Der Betriebsrat kann dies auch einseitig verlangen, da es sich in diesem Fall um zwingende Mitbestimmung sowohl nach dem Betriebsverfassungsgesetz als auch im öffentlichen Dienst nach den Personalvertretungsgesetzen des Bundes und der Länder handelt.

Auch beim Erbringen von VoIP-Dienstleistungen ausschließlich innerhalb der eigenen Firma sind die Vorschriften des § 109 I TKG zu beachten. Danach sind Vorkehrungen zum Schutz des Fernmeldegeheimnisses und personenbezogener Daten sowie Schutzmaßnahmen gegen unerlaubte Zugriffe zu treffen. Sowohl das Fernmeldegeheimnis als auch der Schutz personenbezogener Daten beschränken sich nicht auf den Schutz gegen Angriffe von außen, sondern die Gesprächsverbindungen und die dabei anfallenden personenbezogenen Daten sind auch gegen unbefugte Kenntnisnahme innerhalb des eigenen Unternehmens oder der eigenen Behörde zu schützen.

Dazu sollte daran gedacht werden, die Gesprächsverbindungen vor Zugriffen aus dem Datennetz ausreichend zu sichern. Geeignete Maßnahmen dafür sind die Trennung des Sprach- und des Datennetzes durch komplette Netztrennung, VLAN-Technologie und/oder die komplette Verschlüsselung der Signalisierungs- und/oder Gesprächsdaten. Bei der gemeinsamen Verwendung von Bandbreite mit Datennetzen ist auf ausreichende Priorisierung der Sprachdatenpakete zu achten, um Gesprächsabbrüche zu verhindern. Welche Sicherungsmaßnahmen zum ausreichenden Schutz vor unbefugten Mithörern oder Mitlesern getroffen werden müssen, ist abhängig von der Schutzbedürftigkeit der Daten, da das Telekommunikationsgesetz ähnlich wie die Datenschutzgesetze nur einen Schutz in angemessenem Umfang verlangt.

Werden Telekommunikationsdienstleistungen für einen nicht von vornherein abgrenzbaren Kreis von Nutzern, also Telekommunikationsdienstleistungen für die Öffentlichkeit erbracht, dann sind zusätzlich weitere Sicherheitsmaßnahmen erforderlich. In diesem Fall ist ein Sicherheitsbeauftragter zu bestellen und ein TK-Sicherheitskonzept vorzulegen, das von der Bundesnetzagentur geprüft wird. Diese Sicherheitsmaßnahmen sind aber auch jedem anderen Betreiber eines VoIP-Netzes zu empfehlen.

Bei computergestützter Telefonie sind die zentralen TK-Netzbestandteile gegen Einsichtnahme und gegen Beeinträchtigung zu schützen. Das heißt, dass die Vermittlungsrechner der VoIP-TK-Anlage besonders durch Zutrittsbeschränkungen zu Räumen mit Vermittlungsservern bzw. Voip-TK-Anlagen geschützt werden müssen.
Zusätzlich müssen für die Verfügbarkeitskontrolle nach Datenschutzrecht Maßnahmen gegen die unbefugte Störung der Anlage getroffen werden. Dazu gehört neben dem Schutz des Netzwerks selbst durch Firewalls auch der Schutz gegen Umwelteinflüssen und der Schutz vor Entzug von Versorgungseinrichtungen wie Strom- oder Klimaversorgung. Um den kompletten Ausfall des Netzes bei Stromausfall zu verhindern sollten sowohl die zentralen Einrichtungen mit einer unterbrechungsfreien Stromversorgung ausgestattet sein als auch einzelne Telefone der Vermittlung mit einer von der TK-Anlage unabhängigen Stromversorgung und einem von der VoIP-Anlage unabhängigen PSTN-Anschluss versehen sein, um die telefonische Erreichbarkeit des Unternehmens bzw. der Behörde zu gewährleisten. Bei hohen Verfügbarkeitsanforderungen müssen weitere Sicherheitsmaßnahmen bis hin zur redundanten Bereitstellung einer zweiten VoIP-Anlage in einem weiteren Rechenzentrum.

Für den Fall eines Absturzes müssen wie bei herkömmlichen TK-Anlagen auch Backups der Konfiguration erstellt werden, die im Notfall schnell eingespielt werden können. Bei höherer Verfügbarkeitsanforderung sollte entsprechende Hardware für Notfälle bereitgehalten werden, um ausfallende Bauteile schnell ersetzen zu können.

Administratoren, die eine VoIP-TK-Anlage betreuen sollen, sind besonders mit den Bestimmungen des Datenschutzrechts vertraut zu machen, um die erweiterten Anforderungen von Datenschutz und Fernmeldegeheimnis durch die erweiterten Leistungsmerkmale eines VoIP-Netzes richtig behandeln zu können.
Darüber hinaus ist auf Datenschutzanforderungen bei bestimmten Diensten und Leistungsmerkmalen zu achten. Telefonanrufe bei sozialen Beratungsdiensten, die anonym in Anspruch genommen werden können, sollen nicht durch Einträge in Einzelverbindungsnachweisen nachweisbar sein, daher sind die Nummern, die in einer Liste eingetragen sind, die bei der Bundesnetzagentur geführt wird, in Einzelverbindungsnachweisen komplett zu streichen.

Die Verarbeitung von Verbindungsdaten ist nur zulässig, wenn diese zur Abrechnung von zulässigen Privatverbindungen erforderlich ist. Ansonsten ist die Verarbeitung von Verbindungsdaten im Unternehmen nur zulässig, wenn die Zustimmung des Betriebsrates oder des Personalrates im öffentlichen Dienst vorliegt.

Zur Beantragung eines Einzelverbindungsnachweises für einen Betrieb ist nach dem Telekommunikationsgesetz erforderlich, dass die Zustimmung der Mitarbeiter bzw. der Mitarbeitervertretung vorliegt.

Es gibt jedoch auch zahlreiche Funktionen von Endgeräten oder von zugehörigen CTI-Programmen am PC, die datenschutzrelevant sind.

Die Anruflisten im Telefon können bei Voip-Geräten oder CTI-gestützten PC-Programmen sehr lange Zeiträume umfassen. Da es sich hier um Möglichkeiten der

Leistungsüberwachung handelt, muss dies auch mit der Mitarbeitervertretung besprochen werden.

Gegen Kenntnisnahme Dritter sollte der Abruf der Daten sowohl von den Endgeräten als auch von der zentralen Servern bzw. TK-Anlagen besonders gesichert sein.

Gleiches gilt für das teamweise Signalisieren von Anrufen bei einzeln zugewiesenen Durchwahlen oder der Anzeige in CTI-Programmen anderer Mitarbeiter.

Anrufbeantworterfunktionen sollten beim Abrufen bzw. Administrieren von Nachrichten durch eine PIN gesichert werden.

Es sollte sichergestellt werden, dass es nur nach Absprache mit den Mitarbeitern und mit Zustimmung des Betriebsrates Möglichkeiten gibt, Gespräche aufzuzeichnen und dies nur, wenn es aus überwiegenden betrieblichen Gründen erforderlich ist (z.B. Callcenter). Dabei muss jeweils der Gesprächspartner zu Beginn des Gespräches informiert werden und der eigene Mitarbeiter sollte diese Funktion auf Hinweis des Gesprächspartners deaktivieren können. Es darf keinerlei heimliche Aufzeichnung von Telefonaten geben, da auch das Mithören von dienstlichen Telefonaten durch den Arbeitgeber laut einer Entscheidung des Bundesverfassungsgerichtes ohne Einwilligung nicht zulässig ist.

Persönliche Adressbücher sollten auch nur mit expliziter Genehmigung des Mitarbeiters von anderen einsehbar gemacht werden.

Eine Durchsagefunktion, die ohne Annahme des Empfängers funktioniert, kann auch dazu verwendet werden, unbemerkt den Raum des Telefons zu überwachen, in dem die Durchsage freigeschaltet ist.

Bei der Nutzung von CTI-Funktionen ist darauf zu achten, dass nicht über eine TAPI-Schnittstelle oder ähnliche Schnuttstellen Informationen ähnlich zu den genannten Leistungsmerkmalen von den Mitarbeitern unbemerkt durch das Unternehmen gespeichert werden können.

Mitarbeiter können freiwillig solche Funktionen aktivieren, ansonsten sollten solche Funktionen durch eine Betriebs- oder Dienstvereinbarung abgesichert werden. Freiwilligkeit sollte hier nicht durch Gruppendruck ausgehebelt werden können.

Die Dienstvereinbarung sollte beim Ausbau der Funktionalität einer TK-Anlage regelmäßig angepasst werden, da es sich um zwingende Mitbestimmung handelt. Der Betriebsrat wird in der Regel darauf bestehen, dass die Funktionen der TK-Anlage nicht zur Leistungs- und Verhaltenskontrolle genutzt werden.

Sofern Softphones zur Verwendung an Voip-TK-Anlagen zugelassen werden, sind erheblich erweiterte Datenschutzgefahren vorhanden. Durch jeden PC als Endgerät können selbst verschlüsselte Telefonate quasi unbemerkt mitgeschnitten werden, ohne dass der andere Gesprächspartner davon etwas mitbekommt. Eine solche Vorgehensweise ist jedoch nach § 201 StGB strafbar. Beweismittel, die durch unerlaubtes Mithören gewonnen wurden, unterliegen demzufolge auch einem Beweisverwertungsverbot. Zudem besteht die Gefahr, dass durch Aktivierung von

Videofunktionen der Webcam oder unbemerktes Aktivieren des Mikrophons Raumüberwachungsfunktionen unbemerkt genutzt werden.

Auf der anderen Seite muss der Betreiber von Telekommunikationsanlagen auch darauf achten, dass er alle Auflagen von staatlichen Behörden in Richtung Inhaltskontrolle bzw. Datenspeicherung für Zwecke der Gefahrenabwehr oder der strafrechtlichen oder geheimdienstlichen Ermittlungen erfüllt bzw. argumentieren können, warum die jeweiligen Überwachungsvorschriften im konkreten Fall nicht anwendbar sind.

Bestands- und Gesprächsdaten müssen von Betreibern von öffentlichen Telekommunikationsdiensten für Endnutzer auf Anforderung von Sicherheitsbehörden erfasst werden, bei Vorliegen von schweren Straftaten oder Straftaten, die mittels Telekommunikation begangen wurden, ist auch eine Inhaltskontrolle zulässig. Dabei müssen Kopien sämtlicher Telefonate eines bestimmten Anschlusses mitgeschnitten werden. Diese Vorschriften sind jedoch nicht anwendbar, wenn kein öffentliches TK-Netz für eine geschlossene Anzahl von Benutzern betrieben wird. Das bedeutet, dass interne Gespräche oder deren Logdaten nicht aufgezeichnet werden müssen. Schwieriger wird es bei Privatgesprächen, hier stellt sich die Frage, ob hier Telefondienste für Dritte erbracht werden und damit diese Privilegierung wieder aufgehoben wird. Daher sollten mit den Mitarbeitern bei eigenem Betrieb eines VoIP-Netzes und vor allem beim Betrieb eines VoIP Netzes gemeinsam mit oder für andere Firmen oder Organisationen auch Vereinbarungen geschlossen werden, wie mit der Protokollierung umzugehen ist und gegebenenfalls Betriebs- oder Dienstvereinbarungen geschlossen werden.

Schwierig ist für größere Voip-Netze die Notruffunktionalität zu realisieren. Nach der vom Bundeswirtschaftsministerium erlassenen Notrufverordnung muss jeder, der an Telefondiensten mitwirkt, dem Netzbetreiber den Standort des Notrufs auf technischem Weg mitzuteilen. Dies kann sich bei verteilten Standorten eines VoIP-Netzes als schwierig erweisen. Noch schwieriger wird es, wenn das Voice over IP-Netz über verschiedene Übergänge in das leitungsgebundene Telefonnetz verfügt.

Es ist angesichts der Fülle von Datenschutzthemen im Zusammenhang mit Voip-TK-Anlagen dringend anzuraten, vor der Migration zu einer VoIP-Telefonanlage auch die datenschutzrechtlichen Aspekte zu prüfen und mit dem Datenschutzbeauftragten, dem Betriebsrat und ggf. einem externen Berater zu diskutieren.

Ulrich Emmert,
Partner der esb Rechtsanwälte Partnerschaftsgesellschaft
Lehrbeauftragter an der Hochschule für Wirtschaft und Umwelt
Vaihinger Str. 153
70567 Stuttgart
ulrich.emmert@kanzlei.de
www.kanzlei.de
www.emmert.de