



White Paper: Abwehr von „Spam over Internet Telephony“ (SPIT-AL)

Thomas Rohwer / Carsten Tolkmit,
TNG – THE NET GENERATION AG

Marit Hansen / Markus Hansen /
Jan Möller,
Unabhängiges Landeszentrum für
Datenschutz Schleswig-Holstein
(ULD)

Henning Waack, TU Dresden

Kiel, 31.01.2006
<spital-comment@tng.de>

Das Projekt SPIT-AL wird im Rahmen der Förderung aus dem regionalen Landesprogramm Schleswig-Holstein „e-Region PLUS“ mit Mitteln des Europäischen Fonds für regionale Entwicklung (EFRE) sowie mit Landesmitteln gemäß Antrag vom 31.03.2005 mit den Ergänzungen vom 15.07.2005 unterstützt. Der Förderzeitraum liegt in den Jahren 2005 und 2006.

Executive Summary

Geringe, oft zu vernachlässigende Kosten für Nachrichtenübertragung im Internet haben zu einem starken Aufkommen von unerwünschten Nachrichten (Spam) wie zum Beispiel Werbe-E-Mails, geführt. Mittlerweile ist der Anteil von Spam am gesamten E-Mail-Aufkommen so hoch, dass der Nutzwert des Mediums an sich in Frage gestellt ist. Spam-Filter sollen helfen, das Problem in den Griff zu bekommen.

Mit Voice-over-IP (VoIP) verlagert man die Telefonie auf Datennetze, insbesondere das Internet. Dieser Schritt soll zu Kosteneinsparungen führen.. Experten sagen jedoch voraus, dass mit einer zunehmenden Nutzung und Verbreitung von VoIP auch der Anteil der Spam-Anrufe, sog. SPIT (Spam over Internet Telephony), steigen wird. SPIT-Filter sollen auch hier dem Problem abhelfen.

In dem Projekt SPIT-AL (SPIT-Abwehr-Lösung), das im Rahmen des e-Region PLUS-Programms gefördert wird, erarbeitet der Kieler Internet-Provider TNG – THE NET GENERATION AG mit Unterstützung durch das Unabhängige Landeszentrum für Datenschutz Schleswig-Holstein eine rechtskonforme Lösung für einen einsatzbereiten SPIT-Filter, der in Abhängigkeit der Anruferkennungen verschiedene Reaktionen ermöglichen soll. Dies kann z.B. die Anrufannahme, die Abweisung, eine Umleitung auf die Voicebox oder der Verweis auf eine kostenpflichtige Alternativtelefonnummer sein. Damit soll der Angerufene nicht nur vor unerwünschten Werbeanrufen geschützt, sondern auch in seinem Erreichbarkeitsmanagement unterstützt werden.

Normen aus dem Telekommunikationsrecht, dem Datenschutzrecht und je nach Einsatzumfeld weiteren Rechtsgebieten regulieren die Filterung von Kommunikation im allgemeinen und Telefonie im besonderen. Grundlegende Prinzipien wie eine größtmögliche Transparenz und die nutzerbestimmte Kontrolle der Filterung müssen daher bei der Gestaltung einer SPIT-Abwehrlösung Berücksichtigung finden.

Ziel des White Papers ist – basierend auf den vorgestellten technischen und juristischen Überlegungen – die Entwicklung einer Lösung, die bei Einhaltung aller rechtlichen Vorgaben sowohl eine hohe Filtergenauigkeit als auch Komfort für den Nutzer bietet. Kernstück der Lösung sind White- und Blacklists in einer verteilten Realisierung, anhand derer die Anruferkennungen klassifiziert werden. Zusammen mit weiteren Informationen, zum Beispiel statistischen Bewertungen, ergibt sich daraus, wie der Anruf zu behandeln ist.

Die Autoren laden ein, zu dem vorgestellten Konzept konstruktive Rückmeldungen zu geben, die dann in den weiteren Entwicklungs- und Implementierungsprozess einfließen können.

Inhaltsverzeichnis

1	Einleitung.....	6
2	SPIT-Szenarien und Lösungsansätze.....	8
2.1	Begriffsfestlegungen.....	8
2.1.1	Internettelefonie/Voice-over-IP.....	8
2.1.2	Spam/SPIT.....	8
2.1.3	Spammer.....	8
2.1.4	Kommunikationsidentität.....	8
2.1.5	Verkehrsdaten.....	8
2.2	SPIT-Szenarien.....	9
2.2.1	Call-Center.....	9
2.2.2	Maschinen/Computer.....	9
2.2.3	Mischformen.....	10
2.2.4	Lösungsansätze.....	10
2.2.4.1	Kosten für Telefonie.....	10
2.2.4.2	Buddylists / Whitelists.....	11
2.2.4.3	Erweiterte Whitelist mit Vertrauensnetz.....	11
2.2.4.4	Blacklists.....	11
2.2.4.5	Statistische Blacklist.....	11
2.2.4.6	Voicemenü.....	12
2.2.4.7	Greylists.....	12
2.2.4.8	Gesprächssimulation.....	12
3	Technische Struktur des SPIT-AL-Konzepts.....	13
3.1	Grundsätzliche Funktionsweise.....	13
3.2	Systemarchitektur.....	13
3.3	Features und Funktionsdetails.....	14
3.3.1	Bewertungskriterien in Bezug auf SPIT.....	15
3.3.1.1	Anrufherkunft.....	15
3.3.1.2	Private Whitelist.....	15
3.3.1.3	Importierte Whitelists.....	15
3.3.1.4	Private Blacklist.....	16
3.3.1.5	Importierte Blacklists.....	16
3.3.1.6	Statistische Blacklist.....	16
3.3.2	Maßnahmen.....	16
3.3.2.1	Annahme.....	17
3.3.2.2	Ablehnung/Verwerfen.....	17
3.3.2.3	Weiterleitung an dritten Anschluss.....	17
3.3.2.4	Temporär ablehnen / Greylisting.....	17
3.3.2.5	Ansage mit Hinweis auf alternativen Gesprächsaufbau.....	17
3.3.2.6	Voicemenü.....	17
3.3.2.7	Voicebox.....	17
3.3.3	Weitere Features.....	18
3.3.3.1	Automatische Aufnahme von Kommunikationsidentitäten angerufener Partner in die private Whitelist.....	18
3.3.3.2	Aufzeichnung der Verbindungs- und Entscheidungsdaten.....	18
3.3.3.3	Kennzeichnung laufender Gespräche per Tastencodes.....	18
3.4	Grundsätzliche technische Probleme.....	18
3.4.1	Identitätsunterdrückung.....	18

3.4.2 Identitätsverifikation.....	19
4 Rechtliche Aspekte.....	20
4.1 Grundlagen.....	20
4.1.1 Verfassungsrecht.....	20
4.1.2 Telekommunikationsrecht.....	20
4.1.3 Datenschutzrecht.....	21
4.1.4 Telediensterecht.....	22
4.1.5 Strafrecht.....	22
4.1.6 Verwaltungsrecht.....	22
4.2 Betrachtung ausgewählter Lösungsansätze.....	23
4.2.1 Identifikation von SPIT.....	23
4.2.1.1 Anrufherkunft.....	23
4.2.1.2 Private Whitelist.....	23
4.2.1.3 Private Blacklist.....	23
4.2.1.4 Statistische Blacklist.....	24
4.2.2 Maßnahmen.....	24
4.2.2.1 Annahme von Anrufen.....	24
4.2.2.2 Ablehnung.....	24
4.2.2.3 Weiterleitung an dritten Anschluss.....	24
4.2.2.4 Temporär ablehnen / Greylisting.....	25
4.2.2.5 Ansage mit Hinweis auf alternativen Gesprächsaufbau.....	25
4.2.2.6 Voicemenü.....	25
4.2.2.7 Voicebox.....	25
4.3 Gestaltungsoptionen.....	26
4.3.1 Nutzerkontrollierte Filterung.....	26
4.3.2 Transparenz und Kontrolle der Datenverarbeitung und ihrer Folgen.....	26
4.3.3 Voreinstellungen für verschiedene Nutzergruppen.....	27
5 Zusammenfassung und Ausblick.....	28
6 Literatur.....	29

1 Einleitung

Internettelefonie hat mittlerweile einen technischen Reifegrad erreicht, der eine kostengünstige Nutzung der Voice-over-IP-Telefonie auch für professionelle Ansprüche ohne technisches Detailwissen ermöglicht. Die CeBIT 2005 feierte Voice-over-IP (VoIP) als eine der Schlüsseltechnologien der kommenden Jahre; auch auf der CeBIT 2006 wird VoIP weiterhin Schwerpunkt sein. Die Transformation der klassischen verbindungsorientierten TK-Plattformen in eine paketorientierte Kommunikationswelt (NGN – Next Generation Network) schreitet schnell voran. Insbesondere für kleine und mittlere Unternehmen werden durch die Internettelefonie neue wirtschaftliche Impulse erwartet, denn VoIP macht Telefonieren nicht nur billiger, sondern auch flexibler.

Ähnliche Impulse sind auch mit der massenhaften Verbreitung von E-Mail als geschäftliches wie privates Kommunikationsmedium einhergegangen. Der Nutzwert von E-Mail hat sich mit steigendem Aufkommen unerwünschter Nachrichten (Spam), vor allem der unverlangt eingehenden Werbe-E-Mails, drastisch reduziert. Da das Verschicken von Massen-E-Mails dem Absender kaum Kosten beschert, die über die in der Regel schon vorhandene Infrastrukturanbindung hinausgehen, hat Spam über die Jahre immer weiter zugenommen. Derselbe Effekt wird auch für die Internettelefonie erwartet: Kostenlose Werbe-Anrufe, die auch automatisiert per Sprachcomputer in großem Stil erfolgen können und andere Formen des sog. SPIT (Spam over Internet Telephony) belästigen massenhaft die Nutzer. Rechtliche Regelungen werden wie auch beim Spam nur beschränkten Schutz in Form von Sanktionsmöglichkeiten bieten. Ein Abschreckungseffekt wird davon nur ausgehen, wenn eine effektive Rechtsdurchsetzung gewährleistet werden kann, die oft an Ländergrenzen scheitert. .

Experten erwarten bei zunehmender Verbreitung der Internettelefonie eine ähnliche SPIT-Quote wie bei E-Mail-Spam, der bereits mehr als zwei Drittel aller weltweit versandten E-Mails ausmacht (siehe beispielsweise Spam-Report des Center for Democracy & Technology, 2005). Regulatorische Maßnahmen des deutschen oder europäischen Gesetzgebers haben ebenso wie bei der Spam-Bekämpfung wenig Erfolgsaussichten, weil SPIT genau wie Spam mehrheitlich aus dem Ausland nach Deutschland gelangen wird und dort eine Durchsetzung der deutschen (bzw. europäischen) Vorschriften fehlschlägt.

Abhilfe können SPIT-Filter bieten, die die Erreichbarkeitssphäre der Kunden vor Belästigungen schützen und so den Nutzen der Internettelefonie stärken. Das im Rahmen des schleswig-holsteinischen Programms „e-Region PLUS“ der Europäischen Union geförderte Projekt SPIT-AL (SPIT-Abwehr-Lösung) hat sich zum Ziel gesetzt, einen datenschutzgerechten SPIT-Filter zu konzipieren, zu entwickeln und die programmierte Software unter einer Open Source-Lizenz anzubieten.

Zum White Paper

Dieses White Paper vereint technische und juristische Aspekte zum Themenkomplex SPIT-Abwehr, um gleichermaßen technisch realisierbare und rechtlich einwandfreie Lösungen zu erreichen. Ein besonderer Fokus liegt auf Datenschutz und Datensicherheit, da die Berücksichtigung dieser Thematik nach Einschätzung der Autoren wesentlich für die Akzeptanz einer SPIT-Abwehrlösung durch den Kunden ist.

Das White Paper ist wie folgt aufgebaut: Nach diesem einführenden Kapitel veranschaulichen Szenarien in Kapitel 2 die SPIT-Problematik und zeigen verschiedene Lösungsansätze auf. Die Lösung, die im SPIT-AL-Projekt verfolgt wird, beschreibt das Kapitel 3 in detaillierterer Form: Hier finden sich eine Skizze der Systemarchitektur sowie eine Auflistung von – teilweise optionalen – Features der SPIT-Abwehrlösung. Daran schließt sich in Kapitel 4 die Darstellung der juristischen Grundlagen an, ergänzt um eine Betrachtung einiger ausgewählter Lösungsansätze sowie das Aufzeigen von Gestaltungsoptionen. Das letzte Kapitel fasst das White Paper zusammen und gibt einen Ausblick zu SPIT-Abwehrlösungen mit Fokus auf das Vorgehen im Projekt SPIT-AL.

Das White Paper ist das Basisdokument für das SPIT-AL-Projekt, das für die weitere Spezifikation der zu entwickelnden Lösung verfeinert und ergänzt wird. Mit seinem kombinierten technisch-juristischen Ansatz adressiert es den Bereich der angewandten Forschung und Entwicklung von VoIP und Spam-Abwehr.

Dieses White Paper richtet sich an alle interessierten Leser, die sich mit Voice-over-IP – als Privatanutzer oder als Organisation – beschäftigen. Dies schließt Anwender ebenso ein wie Forscher aus dem technischen oder juristischen Bereich, die sich für praktisch erfolgversprechende und rechtskonforme Methoden der SPIT-Bekämpfung interessieren.

Ganz im Sinne der Open Source-Philosophie sind alle Leser aufgefordert, die vorgestellten Konzepte und Schlussfolgerungen zu kommentieren und zu diskutieren. Verbesserungsvorschläge sind stets willkommen und können per E-Mail gesendet werden an <spital-comment@tng.de>.

2 SPIT-Szenarien und Lösungsansätze

In diesem Abschnitt werden zunächst einige zentrale Begriffe erläutert. Dann werden SPIT-Angriffsszenarien, das heißt die verschiedenen Möglichkeiten zur Verteilung von automatisierten Werbeanrufen über VoIP, und potenzielle Abwehrmechanismen vorgestellt.

2.1 Begriffsfestlegungen

2.1.1 Internettelefonie/Voice-over-IP

Unter Internettelefonie wird im Folgenden ein Sprachtelefondienst über das Internet bezeichnet. Dieser Dienst kann über Peer-to-Peer-Beziehungen oder über einen Anbieter erbracht werden. Typischerweise wird dies mit Hilfe von Voice-over-IP-Technik realisiert. Deshalb wird der Begriff Voice-over-IP zum Teil synonym mit Internettelefonie benutzt. Es soll aber betont werden, dass Voice-over-IP in diesem Dokument nicht als reine Zugangstechnologie zum klassischen Telefonnetz mit einer weitgehend reglementierten Anbieterstruktur verstanden wird.

2.1.2 Spam/SPIT

Als Spam werden unerwünschte Nachrichten im Internet, insbesondere Werbung, bezeichnet; SPIT steht für „Spam over Internet Telephony“, also unerwünschte Nachrichten über Voice-over-IP-Techniken. In diesem White Paper wird der Begriff SPIT jedoch ebenfalls für Werbung aus klassischen Telefonnetzen verwendet.

2.1.3 Spammer

Als Spammer wird der Versender von unerwünschten Nachrichten bezeichnet.

2.1.4 Kommunikationsidentität

Als Kommunikationsidentität wird eine (in der Regel alphanumerische) Zeichenkette bezeichnet, die einen Teilnehmer am Telefonnetz kennzeichnet. Diese Kennung kann zum Beispiel eine Rufnummer oder eine SIP-Adresse sein. Die Anruferidentität beschreibt die Kennung des Initiators einer Telefonverbindung.

2.1.5 Verkehrsdaten

Verkehrsdaten sind gem. § 96 Abs. 1 TKG die Nummer oder Kennung der beteiligten Anschlüsse oder der Endeinrichtung, personenbezogene Berechtigungskennungen, bei Verwendung von Kundenkarten auch die Kartenummer, bei mobilen Anschlüssen auch die Standortdaten, der Beginn und das Ende der jeweiligen Verbindung nach Datum und Uhrzeit und, soweit Entgelte davon abhängen, die übermittelten Datenmengen, der vom Nutzer in Anspruch genommene Telekommunikationsdienst, die

Endpunkte von festgeschalteten Verbindungen, ihr Beginn und ihr Ende nach Datum und Uhrzeit und, soweit die Entgelte davon abhängen, die übermittelten Datenmengen und sonstige zum Aufbau und zur Aufrechterhaltung der Telekommunikation sowie zur Entgeltabrechnung notwendige Verkehrsdaten.

2.2 SPIT-Szenarien

Die hier beschriebenen Szenarien sind unter Umständen nicht beschränkt auf die Internettelefonie; ihre Realisierung ist in näherer Zukunft in diesem Kontext aber am wahrscheinlichsten.

Telefonieprotokolle von modernen Telefonieplattformen (zum Beispiel Internettelefonie) enthalten nicht selten Mechanismen zur Anfrage von Kontextinformationen: So ist es zum Beispiel möglich, den Anwesenheitsstatus des Gegenüber zu erfragen und dabei zusätzlich eine sehr kurze Nachricht zu übertragen, die sich auch für Werbung nutzen ließe. Genauso ist es möglich, Kurznachrichten oder Instant Messages zu verschicken, die als Transportkanal für unverlangte Werbung verwendet werden könnten.

Natürlich kann auch mittels Sprachübertragung der Telefonie geworben werden. Im Folgenden werden einige denkbare Wege aufgeführt.

2.2.1 Call-Center

In einem Call-Center sitzen Telefonisten, die Werbegespräche durchführen. Ein Computer ruft – nach System oder auch wahllos – Telefonierteilnehmer an. Nimmt einer das Gespräch an, wird er an einen freien Telefonisten weitergestellt. Für den Betreiber dieser Art der Telefonwerbung bedeutet dies Kosten für seine Angestellten, für die Computerhardware und gegebenenfalls für jeden zustande gekommenen Telefonanruf (im Internettelefoniebereich werden diese Kosten aber nur eine kleine oder gar keine Rolle spielen). Die Anzahl der gleichzeitig geführten Gespräche – und damit die Spam-Belastung – hängt in erster Linie von der Anzahl der beschäftigten Mitarbeiter ab.

2.2.2 Maschinen/Computer

Gerade Internettelefonie ist eine stark von Computern abhängige Kommunikationsform. So ist es denkbar, dass Computer – nach System oder wahllos – Telefonierteilnehmer anrufen, um ihnen eine festgelegte Werbenachricht vorzuspielen oder sie in eine interaktive Anwendung („Drücken Sie Taste 2, um mehr über uns zu erfahren ...“) einzubinden. Telefonisten sind für diese Art der Werbegesprächs-führung zunächst einmal nicht notwendig.

Für den Betreiber verursacht diese Art der Telefonwerbung in erster Linie Kosten für Computerhardware und für die Kommunikationsanbindung (zum Beispiel Internetanbindung). Ein Großteil der Kosten – nämlich diejenigen für anrufendes Personal – fällt weg. Heutige Preise von Internetanbindungen oder Serverhosting lassen auf diese Weise preisgünstig eine große Anzahl

paralleler Werbetelefonate zu. Niedrige Kosten bei quantitativ hohem Wirkungsgrad könnte die Spam-Belastung durch diese Art von Werbungen erheblich steigern lassen.

2.2.3 Mischformen

Auch Mischformen aus den beiden genannten Szenarien für Sprach-Spam sind denkbar. Die Kosten für den Betreiber werden sich dabei aller Wahrscheinlichkeit nach zwischen den Kosten der beiden Szenarien für Sprach-Spam bewegen.

2.2.4 Lösungsansätze

Je nach Art des Spams kommen verschiedene Möglichkeiten in Frage, den Spam einzudämmen. Im Folgenden werden mögliche Lösungsansätze diskutiert.

Protokoll-Spam (zum Beispiel das Ausnutzen von VoIP-Protokoll-Funktionen wie die Erreichbarkeitsanfrage) wird wahrscheinlich nicht zu einer großen Spam-Belastung führen, da der Nachrichteninhalte, der verschickt werden kann, sehr begrenzt ist und auch die gestalterischen Möglichkeiten zu stark eingeschränkt sind, um eine nennenswerte Werbewirkung zu erzielen. Diese Art von Spam betrachten wir daher nicht weiter.

Für Nachrichten-Spam gibt es heute schon sehr wirkungsvolle Abwehrmechanismen, zum Beispiel Buddylists. Da davon auszugehen ist, dass man diese Art der Kommunikation nur mit bereits bekannten und als „freundlich“ eingestuften Partnern durchführen möchte, wird dieser Abwehrmechanismus auch in Zukunft weiter nutzbar sein. Das Versenden von Nachrichten ist allerdings kein mit der Telefonie unmittelbar verknüpfter Bereich, so dass auch diese Werbeform hier nicht weiter untersucht wird.

Für den eigentlichen SPIT gibt es zur Zeit nur wenige oder gar keine Abwehrmechanismen, und der Anteil dieser Art von Spam wird voraussichtlich in Zukunft anwachsen. Die hier untersuchte SPIT-Abwehrlösung widmet sich daher der Abwehr der Werbung mittels Sprachtelefonie. Es gibt unter anderem folgende Lösungsansätze, diese Art von Telefonie-Spam abzuwehren oder einzudämmen, wobei Mischformen der genannten Ansätze ebenfalls denkbar sind:

2.2.4.1 Kosten für Telefonie

Ein allgemeiner Ansatz, sich vor unerwünschten Werbeanrufen zu schützen, besteht darin, die Kosten der Anrufe für den Werbeversender zu erhöhen. Dies steht natürlich im Widerspruch zu der mit der Internettelefonie erhofften Kosteneinsparung. Trotzdem kann dieses Verfahren als Ergänzung sinnvoll sein, um bei unbekanntem Anrufer, die sonst abgelehnt würden, eine initiale Kontaktaufnahme zu höheren Kosten zu ermöglichen, zum Beispiel indem man auf einen Zugang über das klassische Telefonnetz verweist oder den Anrufer eine Aufgabe (siehe Abschnitt 2.2.4.6) lösen lässt.

2.2.4.2 Buddylists / Whitelists

Jeder Telefonieteilnehmer führt eine Liste von Teilnehmern, von denen er Anrufe entgegen nehmen möchte. Dritt-Teilnehmer, die nicht auf dieser Liste sind, können den Anschlussinhaber nicht anrufen. Dies führt zu Problemen bei der initialen Kontaktaufnahme. Dieser Mechanismus ist zwar gut geeignet, SPIT abzuwehren, allerdings wehrt er auch mit großer Wahrscheinlichkeit erwünschte Anrufe ab. Telefonie wäre bei ausschließlicher Verwendung von Whitelists als Medium für den Erstkontakt nicht mehr geeignet. Als ein Teil der SPIT-Abwehrlösung könnte jedoch ein diesem System sehr ähnliches Verfahren zum Einsatz kommen.

2.2.4.3 Erweiterte Whitelist mit Vertrauensnetz

Damit man auch von Anrufern, die nicht auf der eigenen Whitelist stehen, angerufen werden kann, könnte man auf ein Vertrauensnetz zurückgreifen; Jeder Teilnehmer spricht einigen anderen Teilnehmern sein Vertrauen aus und profitiert dann von den Einträgen in deren Whitelists, indem er Anrufe von Teilnehmern auf deren Whitelists auch direkt zulässt. Wenn diese Whitelists über mehrere Schritte von Vertrauten und Vertrauten von Vertrauten weitergereicht würden, könnten bereits eine deutlich höhere Anzahl von Teilnehmern den Anschlussinhaber ohne Probleme anrufen (Kleine-Welt-Phänomen, Stanley Milgram). Die wesentlichen Probleme der White- oder Buddylist bleiben aber zunächst bestehen: Der Anrufer muss erst einmal auf eine der Whitelists des Vertrautenkreises kommen.

2.2.4.4 Blacklists

Es gibt Listen – entweder führt jeder Teilnehmer seine eigenen, oder aber es gibt eine oder mehrere zentrale –, in denen die Teilnehmer verzeichnet sind, die SPIT verbreiten. Der Anschlussinhaber nimmt dann nur noch Gespräche an, die auf keiner Blacklist verzeichnet sind. Leider kann dieses System nur Werbeanrufe abwehren, deren Anruferidentität auf der verwendeten Blacklist verzeichnet – also bekannt – sind. Führt dabei jeder Teilnehmer seine eigene Blacklist, hat also nur seine eigenen Daten über SPIT-Anrufer zur Verfügung, ist es wahrscheinlich, dass die Erkennungsrate für SPIT-Anrufe sehr gering ist. Eine zentrale Blacklist wäre effektiver. Werbeanrufe von noch nicht negativ in Erscheinung getretenen Spammern können Blacklists aber nur beschränkt abwehren.

2.2.4.5 Statistische Blacklist

Aus bestimmten Verkehrsdaten könnte ein Telefonieanbieter mittels statistischer Verfahren Rückschlüsse auf die Natur bestimmter Anrufer ziehen. Wenn zum Beispiel derselbe Teilnehmer in einem gewissen Zeitraum hunderte von verschiedenen Anschlüssen anruft und die resultierenden Gespräche jeweils recht kurz sind, so ist davon auszugehen, dass es sich bei dem Anrufer wahrscheinlich um einen Spammer handelt. So könnte eine Blacklist aufgebaut werden, von der die angerufenen Teilnehmer profitieren, da dieser Spammer für die Zukunft und für andere

Teilnehmer des Telefonieanbieters ausgeschlossen werden kann. Als ein Teil der SPIT-Abwehrlösung könnte dieses System zum Einsatz kommen.

2.2.4.6 Voicemenü

Jeder Anrufer hört zunächst ein Voicemenü, das ihm eine bestimmte Aufgabe stellt (zum Beispiel „Um mit dem Teilnehmer Kontakt aufnehmen zu können, drücken Sie bitte 635#*.“). Erst nach korrekter Erfüllung dieser Aufgabe wird eine direkte Verbindung zum angerufenen Teilnehmer hergestellt. Mit dieser Lösung kann von Maschinen/Computern ausgehender SPIT abgefangen werden, denn die meisten Computer werden – zumindest heute und in naher Zukunft – nicht in der Lage sein, die Aufgaben automatisch zu lösen. Call-Center-SPIT ist hiermit allerdings nicht abzufangen, allerdings ebenfalls durch diese Methode eindämmbar, da die Call-Center-Agents länger brauchen, ein Gespräch aufzubauen, und dies Arbeitszeit und damit Geld kostet. Dieses Verfahren könnte als Teilkomponente in der SPIT-Abwehrlösung zum Einsatz kommen.

2.2.4.7 Greylists

Eine Greylist ist eine Art „unscharfe“ Black- oder Whitelist, deren Verhalten von den Umständen der Anrufe abhängt: Ein Anrufversuch wird dem Anrufer zunächst als „Klingeln“ oder „Besetzt“ signalisiert, ohne dass das Telefon beim Angerufenen klingelt. Erst wenn der Anrufer innerhalb eines gewissen Zeitraumes erneut anruft – es kann dann davon ausgegangen werden, dass es sich um einen Menschen handelt, der ein Interesse daran hat, den anderen wirklich zu erreichen, wird er direkt zum Angerufenen durchgestellt. Dieses Verfahren birgt natürlich das Risiko, dass Anrufcomputer oder -maschinen sich darauf einstellen und ähnlich arbeiten. Als Teilkomponente könnte das Greylist-Verfahren in der SPIT-Abwehrlösung Anwendung finden.

2.2.4.8 Gesprächssimulation

Ähnlich wie bei einem Voicemenü hört der Anrufer eine menschliche Stimme. Die voraufgezeichneten Audio-Daten suggerieren, dass tatsächlich ein menschlicher Gesprächspartner das Gespräch angenommen hat. In Abhängigkeit von Sprechpausen des Anrufers werden mehr oder weniger zusammenhängende gesprochene Sätze eingeworfen. Ziel einer solchen Implementierung ist es, den als Spammer erkannten Anrufer möglichst lange an ein Gespräch zu binden, ohne dass er hinsichtlich seiner Verkaufsabsicht erfolgreich ist. Die Ressourcen des Anrufers werden so gebunden und sein Geschäftsmodell insgesamt weniger rentabel. Dabei ist allerdings zu beachten, dass dies auch auf Seiten des Angerufenen Ressourcen bindet. Für den SPIT-AL-Prototyp ist eine Implementierung nicht vorgesehen.

3 Technische Struktur des SPIT-AL-Konzepts

Aus den beschriebenen Lösungsansätzen ergibt sich die folgende technische Struktur für die Funktion einer SPIT-Abwehrlösung. Außerdem werden ihre Leistungsmerkmale, die Gesamtarchitektur und der Einsatzkontext näher beschrieben.

3.1 Grundsätzliche Funktionsweise

Die SPIT-Abwehrlösung nimmt Telefonanrufe stellvertretend für den Angerufenen entgegen. Dann wird der Anruf aufgrund der Anruf-Metadaten (Anruferidentität, Herkunft, gegebenenfalls Zeitpunkt) und den Präferenzen des Angerufenen bewertet. Eine Auswertung des Voice-Streams, also von Telekommunikationsinhalten, findet hierbei nicht statt, da die Klassifizierung der Anrufe schnell – nämlich vor der potenziellen Belästigung – erfolgen muss. Aus der ermittelten Bewertung entscheidet sich das System, wie der Anruf zu behandeln ist, das heißt, welche Maßnahme (zu den Aktionen siehe 3.3.2) zu ergreifen ist.

3.2 Systemarchitektur

Die SPIT-Abwehrlösung soll möglichst so ausgelegt werden, dass sie per VoIP in eine Telekommunikationsinfrastruktur integriert werden kann. Die Anbindung an PSTN/ISDN und Internettelefonie-Dienste geschieht mit Komponenten, die nicht im Projekt erstellt werden. Der Betreiber der Telefonanlage (oder des Voice-Switches), auf der die Gespräche terminieren, ist dafür verantwortlich, dass Anrufe für Kunden, die an der SPIT-Abwehrlösung teilnehmen wollen, auch zunächst dort ankommen. So kann die SPIT-Abwehrlösung für unterschiedliche Telefoniemedien eingesetzt werden. Für bestimmte Funktionen (zum Beispiel die statistische Filterung) ist eine engere Koppelung an die Infrastruktur des Betreibers notwendig.

Die Architektur des SPIT-AL-Konzepts ist in mehrere funktionale Subsysteme aufgeteilt.

Der *Application-Softswitch* sorgt für das Routing der Anrufe zwischen den einzelnen Komponenten, die verschiedene abgestufte Maßnahmen umsetzen. Teilnehmer, die von der SPIT-Abwehrlösung profitieren wollen, müssen ihre Anrufe zunächst zu diesem System routen.

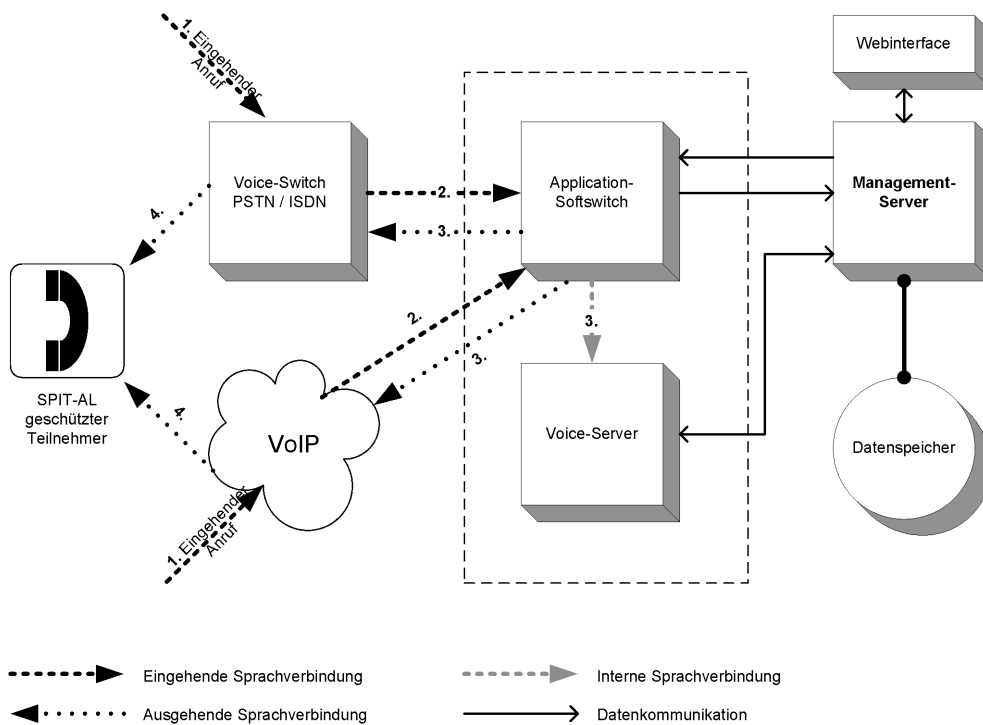
Für die Umsetzung einiger denkbarer Maßnahmen innerhalb der SPIT-AL steht dem Application-Softswitch ein *Voice-Server* zur Seite. Der Voice-Server stellt Funktionen für Voiceboxen, Sprachmenüs oder einfache Ansagen zur Verfügung.

Der Application-Softswitch trifft allerdings selbst keine Entscheidungen über das Routing, sondern greift hierzu auf einen *Management-Server* zurück. Der Management-Server nimmt vom Application-Softswitch Anruf-Metadaten entgegen und liefert daraufhin dem Application-Softswitch eine Entscheidung zurück, zu welchem Ziel der Anruf zu routen ist. Auf dem Management-Server werden auch alle benutzerspezifischen Einstellungen

(Settings, Preferences) und die Daten für die einzelnen Mechanismen (siehe unten) verwaltet.

Der Management-Server legt alle für das System relevanten Daten in einem *Datenspeicher* ab.

Ein *Webinterface* ermöglicht es dem Nutzer, seine Daten (persönliche Einstellungen, White- und Blacklists (siehe unten), gegebenenfalls Voiceboxinhalt) über den Management-Server zu verwalten.



Als Basis für den Application-Softswitch und den Voice-Server könnte die Open-Source-Software Asterisk (<http://www.asterisk.org>) zum Einsatz kommen.

Die einzelnen Subsysteme können sowohl verteilt als auch auf einem einzelnen Rechner zum Einsatz kommen. So kann die SPIT-Abwehrlösung sowohl von Telefonieanbietern als zusätzlicher Service eingebunden als auch innerhalb von Firmen oder Behörden (oder kleinen Privatnetzen) direkt eingesetzt werden.

3.3 Features und Funktionsdetails

Jeder Nutzer der SPIT-Abwehrlösung stellt über das Webinterface seine persönlichen Einstellungen ein. Auf die einzelnen Einstellungen wird im Folgenden noch detailliert eingegangen.

Aus den vom Application-Softswitch übergebenen, bereits bekannten Verbindungsdaten wie Kommunikationsidentität des Anrufers, Herkunft des Anrufes (PSTN, VoIP, aber unter Umständen auch Netzbetreiber des Anrufer-Netzes), Uhrzeit usw. berechnet der Management-Server eine Punktzahl. Dabei können einige der oben erwähnten Nutzereinstellungen eine Rolle spielen. Für bestimmte Intervalle dieser Punktzahlen legt der Nutzer in seinen Einstellungen auch fest, welche Maßnahmen für Anrufe

durchgeführt werden sollen, die mit entsprechenden Punktzahlen bewertet sind.

3.3.1 Bewertungskriterien in Bezug auf SPIT

Im Folgenden werden eine Reihe von Bewertungskriterien zur Einstufung eines Anrufs als mutmaßlicher SPIT aufgeführt, von denen in der SPIT-Abwehrlösung einige ausgewählte zum Einsatz kommen. Zur Berechnung der oben genannten Punktzahl werden in der Regel mehrere verschiedene Kriterien herangezogen und die Ergebnisse der Einzelbewertungen in geeigneter Form miteinander verknüpft (zum Beispiel addiert, gegebenenfalls auch gewichtet).

Nicht alle der hier angegebenen Bewertungskriterien sollen bereits im Prototyp der SPIT-Abwehrlösung realisiert werden. Für die im Projekt verfolgte Lösung werden zunächst die Bewertungskriterien „Private Whitelist“ und „Private Blacklist“ implementiert.

3.3.1.1 Anruferkunft

Ein Anruf kann nach seiner Herkunft klassifiziert werden: Kommt er zum Beispiel aus einem klassischen Telefonnetz (PSTN), so kann dies zu einer positiven Bewertung führen, da davon ausgegangen werden kann, dass Telefongespräche dort höhere Kosten verursachen und deshalb die SPIT-Wahrscheinlichkeit geringer ist.

Auch Anrufe von großen VoIP-Providern mit entsprechend reglementierter VoIP-Infrastruktur – zum Beispiel könnten Werbeanrufe per AGB verboten und technisch unterbunden sein – könnten als solche erkannt werden und zu einer positiven Bewertung führen.

Im Gegensatz dazu könnten Anrufe direkt von Einwahl- oder DSL-Internetanschlüssen zu einer negativen Bewertung führen.

3.3.1.2 Private Whitelist

Jeder Nutzer der SPIT-Abwehrlösung pflegt in seinen Einstellungen eine Liste von Kommunikationsidentitäten, die er kennt und für vertrauenswürdig hält. Steht ein Anruf mit seiner Anruferidentität auf dieser Liste, wird er stark positiv bewertet.

3.3.1.3 Importierte Whitelists

Jeder Nutzer der SPIT-Abwehrlösung kann in seinen Einstellungen festlegen, ob er seine private Whitelist veröffentlichen möchte. Außerdem kann er dort festlegen, von welchen anderen Nutzern er deren veröffentlichte Whitelists mit welcher Gewichtung in sein eigenes System aufnehmen will. Wenn nun ein Anruf mit seiner Anruferidentität nicht auf der eigenen Whitelist steht, so werden die anderen (importierten) Listen befragt; das Ergebnis mit der Gewichtung verknüpft führt so ebenfalls zu einer Punktzahl. Dieser Vorgang kann auch rekursiv geschehen, so dass eine Anfrage – zumindest über eine begrenzte Anzahl von Schritten – an die Freunde des Freundes usw. weitergereicht werden können.

Aus datenschutzrechtlichen Gründen ist es denkbar, diese Lösung um einen (oder mehrere) zentrale(n) Server zu erweitern, in denen die Telefonieteilnehmer zunächst einmal ihre Kommunikationsidentität hinterlegen und damit explizit dem Transfer ihrer personenbezogenen Daten zustimmen müssen. Daten über Teilnehmer, die nicht in einem dieser Verzeichnis-Server abgelegt sind, werden dann auch nicht zwischen Freunden ausgetauscht.

3.3.1.4 Private Blacklist

Jeder Nutzer der SPIT-Abwehrlösung pflegt in seinen Einstellungen eine Liste von Kommunikationsidentitäten, die er kennt und als Spammer identifiziert hat. Steht ein Anruf mit seiner Anruferidentität auf dieser Liste, wird er stark negativ bewertet.

3.3.1.5 Importierte Blacklists

Jeder Nutzer der SPIT-Abwehrlösung kann in seinen Einstellungen festlegen, ob er seine private Blacklist veröffentlichen möchte. Außerdem kann er dort festlegen, von welchen anderen Nutzern er deren veröffentlichte Blacklists mit welcher Gewichtung in sein eigenes System aufnehmen möchte. Wenn nun ein Anruf mit seiner Anrufer-Identität nicht auf der eigenen Blacklist steht, so werden die anderen (importierten) Listen befragt; das Ergebnis mit der Gewichtung verknüpft führt so ebenfalls zu einer Punktzahl. Dieser Vorgang kann auch rekursiv geschehen, so dass eine Anfrage – zumindest über eine begrenzte Anzahl von Schritten – an die Freunde des Freundes usw. weitergereicht werden können.

3.3.1.6 Statistische Blacklist

Die SPIT-Abwehrlösung kann aus den Verkehrsdaten (Anrufer, Angerufener, Zeitpunkt, Dauer) aller durch sie geleiteten Anrufe Statistiken über bestimmte Anrufer erstellen. Wenn ein Anrufer innerhalb kurzer Zeit eine große Menge von Telefonanschlüssen anruft und die meisten dieser Gespräche eine kurze Dauer aufweisen, so kann davon ausgegangen werden, dass der Anrufer ein Spammer ist. Diese Information kann wiederum in einer Blacklist veröffentlicht werden, die die einzelnen SPIT-AL-Nutzer genau wie andere Blacklists importieren können.

3.3.2 Maßnahmen

Hat der Management-Server nun für den einkommenden Anruf eine Punktzahl ermittelt, wird in den Nutzereinstellungen des angerufenen Anschlusses die anzuwendende Maßnahme nachgeschlagen. Im Folgenden werden mögliche Maßnahmen vorgestellt, wobei nicht alle der unten erwähnten Maßnahmen Bestandteil des Prototyps sein werden. Für die SPIT-Abwehrlösung werden zunächst die Maßnahmen „Annahme“, „Ablehnung“ und „Weiterleitung an dritten Anschluss“ implementiert.

3.3.2.1 Annahme

Ein Anruf, der diese Maßnahme zur Folge hat, wird direkt zum Anschlussinhaber durchgestellt. Das Gespräch mit dem Anrufenden kommt also sofort zustande. Bei einer hohen positiven Bewertung (zum Beispiel durch eine private Whitelist) wird der Anrufer direkt zum Angerufenen durchgestellt.

3.3.2.2 Ablehnung/Verwerfen

Dem Anrufer wird ein Klingelsignal (oder ein Nicht-Vorhanden-Sein des angerufenen Anschlusses) signalisiert, beim angerufenen Teilnehmer klingelt es jedoch nicht. Bei einer stark negativen Bewertung (zum Beispiel durch eine private Blacklist) kann der Anrufer den Angerufenen nie erreichen und erhält auch keine Aussage zu dessen tatsächlicher Erreichbarkeit.

3.3.2.3 Weiterleitung an dritten Anschluss

Der Anrufer wird an einen vom Nutzer der SPIT-Abwehrlösung konfigurierten dritten Anschluss weitergeleitet. Dort kann der Angerufene zum Beispiel einen eigenen Anrufbeantworter betreiben oder andere Mechanismen selbst implementieren.

3.3.2.4 Temporär ablehnen / Greylisting

Dem Anrufer wird ein „Besetzt“ signalisiert; sollte er innerhalb einer kurzen Zeit abermals anrufen, wird er direkt durchgestellt. Ruft er innerhalb eines längeren Zeitraumes noch einmal an, wird auf eine andere Maßnahme geschwenkt.

3.3.2.5 Ansage mit Hinweis auf alternativen Gesprächsaufbau

Dem Anrufer wird auf den Voice-Server weiterverbunden, wo ihm eine Ansage vorgespielt wird, in der ihm erklärt wird, wie er mit dem Nutzer Kontakt aufnehmen kann, zum Beispiel durch einen (kostenpflichtigen) Anruf über das klassische Telefonnetz.

3.3.2.6 Voicemenü

Der Anrufer wird auf den Voice-Server weiterverbunden und in ein Sprachmenü umgeleitet, wo er sich eine (gegebenenfalls längere) Ansage anhören oder eine Aufgabe („um direkt mit dem Teilnehmer verbunden zu werden, drücken Sie bitte die 7“) durchführen muss. Danach wird er mit dem Nutzer verbunden.

3.3.2.7 Voicebox

Der Anrufer wird auf den Voice-Server weiterverbunden und kann eine Nachricht in einer Voicebox hinterlassen. Gegebenenfalls muss er davor eine Aufgabe (siehe 3.3.2.6) ausführen.

3.3.3 Weitere Features

Um dem Nutzer die Benutzung der SPIT-Abwehrlösung so einfach wie möglich zu gestalten, kommen weitere Features für die zu implementierende Lösung in Frage:

3.3.3.1 Automatische Aufnahme von Kommunikationsidentitäten angerufener Partner in die private Whitelist

Ruft ein Nutzer der SPIT-Abwehrlösung einen Anschluss an, so kann die Kommunikationsidentität des angerufenen Anschlusses direkt in die private Whitelist des Nutzers aufgenommen werden, da davon auszugehen ist, dass Rückrufe von der angerufenen Person erwünscht sind.

3.3.3.2 Aufzeichnung der Verbindungs- und Entscheidungsdaten

Wird ein Nutzer der SPIT-Abwehrlösung angerufen, werden Verbindungsdaten wie Zeitpunkt, Kommunikationsidentität des Anrufenden ebenso aufgezeichnet wie die durch den Management-Server ermittelte Punktzahl (mit kurzer Erklärung, wie diese Punktzahl zustande kommt).

Im Webinterface, in dem Nutzer seine Einstellungen und privaten Listen pflegt, kann der Nutzer diese Verbindungsdaten dann betrachten und so zum Beispiel mit einem einzelnen Klick einen Anrufer als Spammer oder Freund markieren und ihn somit einer der beiden Listen (White- oder Blacklist) hinzufügen.

Nutzt der SPIT-AL-Teilnehmer die SPIT-AL-eigene Voicebox, können auch dort zu den Anrufen die Metadaten mit aufgeführt werden, und auch dort kann dem Teilnehmer leicht ermöglicht werden, Anrufer als Freunde oder Spammer zu markieren und diesen so in die entsprechenden Listen aufnehmen.

3.3.3.3 Kennzeichnung laufender Gespräche per Tastencodes

Telefoniert ein Nutzer der SPIT-Abwehrlösung mit einem Partner, so kann er während des Gespräches durch bestimmte Tastencodes den Anrufer in seine private White- oder Blacklist aufnehmen.

3.4 Grundsätzliche technische Probleme

3.4.1 Identitätsunterdrückung

Es gibt in der Telefonie die Technik, seine Kommunikationsidentität zu unterdrücken, das heißt der angerufene Partner hat dann keine Möglichkeit, diese zu erkennen. Hierdurch wird die Effizienz der White- und Blacklists reduziert, da keine gesicherte Aussage über die Identität eines Anrufers mit gelisteten Anrufern getroffen werden kann.

3.4.2 Identitätsverifikation

In der Internettelefonie ist die Absenderidentität zur Zeit noch recht leicht fälschbar, und zum gegenwärtigen Zeitpunkt bestehen keine verbindlichen Standards zur Verifikation einer Absenderidentität.

4 Rechtliche Aspekte

Die Ausfilterung von Telefonanrufen in der oben beschriebenen Art wirft eine Reihe rechtlicher Fragen auf, die im Rahmen der Gestaltung einer technischen Abwehrlösung gegen unerwünschte Telefonanrufe zu berücksichtigen sind.

4.1 Grundlagen

Verschiedene Normen aus unterschiedlichen Rechtsgebieten können auf Verfahren, die im Kontext der SPIT-Filterung genutzt werden sollen, regelnd einwirken.

4.1.1 Verfassungsrecht

Hier ist zunächst das Verfassungsrecht zu nennen. Art. 10 Grundgesetz enthält das Fernmeldegeheimnis. Es schützt die Inhalte einer Telekommunikation ebenso wie die Tatsache, dass überhaupt eine Telekommunikation zwischen bestimmten Beteiligten stattgefunden hat. Es verpflichtet die Anbieter von Telekommunikation und deren Mitarbeiter.

Eine detailliertere Ausgestaltung des Fernmeldegeheimnisses findet sich in § 88 Telekommunikationsgesetz (siehe 4.1.2); die strafrechtliche Bewehrung von Verstößen ist § 206 Strafgesetzbuch geregelt (siehe 4.1.5).

Für die oben geschilderte Lösung der Ausfilterung von unerwünschten Anrufen ist das Fernmeldegeheimnis problematisch, da zwar keine Inhalte der Telekommunikation, wohl aber eine Reihe von Verkehrsdaten (siehe oben 2.1.5) automatisiert zur Kenntnis genommen und für die Bewertung eines Anrufs genutzt werden sollen. Die Verkehrsdaten unterfallen zumindest bis zum Abschluss des Übertragungsvorgangs dem Schutz des Telekommunikationsgeheimnisses.

Unproblematisch gestaltet sich Kenntnisnahme und Nutzung von Verkehrsdaten durch an der Telekommunikation Beteiligte. Vor diesem Hintergrund ist es sinnvoll, die vollständige Kontrolle über die SPIT-Abwehrlösung in die Hände des Nutzers zu legen (siehe 4.3.1).

4.1.2 Telekommunikationsrecht

Die SPIT-Abwehrlösung arbeitet in einem telekommunikationsrechtlich regulierten Umfeld. Sowohl Anrufe aus öffentlichen Telekommunikationsnetzen (PSTN) als auch solche, die auf Voice-over-IP-basierten Übertragungswegen übermittelt werden, sollen dem nutzerkontrollierten Anrufmanagement unterliegen. Verpflichtet werden durch das Telekommunikationsrecht die Anbieter von Telekommunikation bzw. insbesondere solche von Telekommunikationsdiensten.

Dies könnte speziell die Betreiber der SPIT-Abwehrlösung betreffen, soweit die Lösung – wie hier vorgesehen – zentral und nicht im Endgerät des Nutzers implementiert ist.

Neben dem bereits genannten in § 88 Telekommunikationsgesetz spezifizierten Telekommunikationsgeheimnis könnten dabei insbesondere die §§ 148f. TKG eine Rolle spielen, soweit mit der Filterung von Anrufen eine Unterdrückung von Nachrichten verbunden wäre. Dies könnte insbesondere bei der direkten Ablehnung von Anrufen (siehe 4.2.2.2), aber auch beim Greylisting (siehe 4.2.2.4) der Fall sein.

Telekommunikationsrechtlich bisher nur in Ansätzen geklärt ist die Einstufung von Voice-over-IP-basierter Sprachtelefonie (vgl. Eckpunkte der regulatorischen Behandlung von VoIP der Bundesnetzagentur).

4.1.3 Datenschutzrecht

Weiterhin beeinflusst auch das Datenschutzrecht die Ausgestaltung der SPIT-Abwehrlösung. Das Datenschutzrecht regelt die Erhebung, Verarbeitung und Nutzung personenbezogener Daten. Als spezialgesetzliche Normen sind hier insbesondere die §§ 91-107 TKG zu berücksichtigen, die besondere Regelungen zum Telekommunikationsdatenschutz enthalten.

Darüber hinaus gilt das Bundesdatenschutzgesetz subsidiär, das heißt soweit das Spezialgesetz keine anderweitige Regelung vorsieht. Grundsätzlich gilt das Datenschutzgesetz nicht für private und familiäre Tätigkeiten. Daraus ergibt sich eine andere Rechtslage für den privaten Einsatz der SPIT-Abwehrlösung als für die geschäftliche Nutzung durch Freiberufler oder Unternehmen oder für den Einsatz in der dienstlichen Kommunikation von Behörden.

Eine zentral beim Telekommunikationsanbieter eingerichtete SPIT-Abwehrlösung wirft die Frage auf, inwieweit dort stattfindende Erhebungen, Verarbeitungen oder Nutzungen personenbezogener Daten noch als privilegierte private oder familiäre Tätigkeit angesehen werden können. Dies könnte angenommen werden, wenn es sich dabei um eine Auftragsdatenverarbeitung gem. § 11 Bundesdatenschutzgesetz handelt. Eine Auftragsdatenverarbeitung mit dem Nutzer als Auftraggeber und dem SPIT-AL-Betreiber als Auftragnehmer setzt neben einem schriftlichen Vertrag insbesondere die Weisungsgebundenheit des Auftragnehmers und eine Kontrollmöglichkeit für den Auftraggeber voraus. Um die datenschutzrechtliche Privilegierung für den privaten Einsatz von SPIT-Bewertungsmechanismen nutzen zu können, ist daher eine vollständige Nutzerkontrolle der Bewertungsmechanismen wie auch der darauf basierenden Maßnahmen mit vorzusehen.

Gleichzeitig ergibt sich aus den unterschiedlichen Rechtsgrundlagen der Ausfilterung die Notwendigkeit, beim SPIT-AL-Einsatz bei Privatpersonen andere Mechanismen zu kombinieren als beim Einsatz in Unternehmen. Weitere Unterschiede können sich für Behörden aus verwaltungsrechtlichen Anforderungen (siehe 4.1.6) ergeben.

Neben der Frage der Verantwortlichkeit für die personenbezogene Datenverarbeitung beim Einsatz der SPIT-Abwehrlösung ist insbesondere deren Zulässigkeit auf Basis einer Einwilligung oder einer gesetzlichen Erlaubnisvorschrift sicherzustellen. In beiden Fällen ist die Transparenz der

Verarbeitung für den Betroffenen und eine Möglichkeit zur Ausübung seines Widerspruchsrechts einzuräumen.

Die rechtlich geforderte Möglichkeit der Unterdrückung der Teilnehmerkennung ist in der Voice-over-IP-basierten Sprachtelefonie zumindest im Hinblick auf die IP-Adresse faktisch nicht zu erfüllen. Die SPIT-Abwehrlösung macht von den so gewonnenen Informationen zur Bewertung von Anrufen Gebrauch. Ob eine solche Nutzung mit dem Sinn und Zweck der Vorschrift zu vereinbaren ist, ist näher zu untersuchen.

4.1.4 Telediensterecht

Um eine vollständige Nutzerkontrolle des Filters transparent und praktisch handhabbar für den Nutzer umsetzen zu können, bietet sich bei einer zentral installierten SPIT-Abwehrlösung das Angebot einer Webschnittstelle zur individuellen Konfiguration durch den Nutzer an. Die Bereitstellung einer solchen Schnittstelle könnte einen Teledienst nach § 2 Abs. 1 Teledienstegesetz darstellen. Dies hat zur Folge, dass unter anderem die formalen Anforderungen des § 6 TDG (Impressumpflicht), aber auch die datenschutzrechtlichen Vorgaben nach dem Teledienstedatenschutzgesetz zu berücksichtigen sind.

Darüber hinaus könnte für die Bewertungsmechanismen verteilter White- und Blacklists eine webbasierte Einwilligungs- und Widerrufinfrastruktur erforderlich sein, um Datenschutzvorgaben zu erfüllen. Eine solche Lösung müsste sich unter anderem hinsichtlich der Anforderungen an eine Einwilligung ebenfalls an den Regelungen des Teledienstedatenschutzgesetzes orientieren.

4.1.5 Strafrecht

Die § 148 TKG und § 206 StGB bewahren Verstöße gegen das Fernmeldegeheimnis (siehe oben 4.1.1 und 4.1.2) mit Geld- oder Freiheitsstrafe. Diese drastische Sanktionsmöglichkeit soll die Durchsetzung der Vorschrift erleichtern und unterstreicht die Hocharrangigkeit des Rechtsguts „Fernmeldegeheimnis“. Da das Grundkonzept der SPIT-Abwehrlösung von einer zentral zum Beispiel beim Telekommunikationsanbieter aufgesetzten Lösung ausgeht, würden sich für diesen durch den Betrieb erhebliche Gefahren bei einem Verstoß ergeben. Dies ist besonders bei der technischen Gestaltung der SPIT-Abwehrlösung als auch der rechtlichen Beziehungen von Nutzer und Betreiber zu berücksichtigen.

4.1.6 Verwaltungsrecht

Soweit ein SPIT-AL-Einsatz auch bei Behörden stattfinden soll, ist bei der Akzeptanz von Anrufen auch die Pflicht zur Gewährung rechtlichen Gehörs zu berücksichtigen. In förmlichen Verwaltungsverfahren, die auch Nachteile für Bürger zur Folge haben können, ist dem Bürger regelmäßig Gelegenheit zur Stellungnahme zu geben. Dabei kann sich der Bürger grundsätzlich aller durch die öffentliche Stelle eröffneten Kommunikationskanäle bedienen. Solche Kanäle sind gem. § 52a Abs. 1 LverwG S-H bzw.

vergleichbarer Vorschriften in anderen Ländern zu eröffnen. Sollte es ihm aufgrund der SPIT-Abwehrlösung nicht möglich sein, seine Erwiderung vorzubringen, könnte dies eine Verletzung rechtlichen Gehörs darstellen. Dies ist bei der Kombination von Mechanismen (siehe Voreinstellungen, 4.3.3) und der grundsätzlichen Frage des Einsatzes der SPIT-Abwehrlösung für behördliche Anschlüsse zu berücksichtigen.

4.2 Betrachtung ausgewählter Lösungsansätze

4.2.1 Identifikation von SPIT

Die Identifikation von SPIT setzt die Auswertung einer Reihe von Kontextdaten des Anrufs voraus, die aufgrund einer Zuordnung zu einer bestimmten Teilnehmerkennung oder IP-Adresse personenbezogen sein können. Ebenso können aus diesen Daten Informationen gewonnen werden, die dem Schutz des Telekommunikationsgeheimnisses unterliegen.

4.2.1.1 Anruferkunft

Die Auswertung der Teilnehmerkennung oder IP-Adresse soll zur Identifikation von SPIT herangezogen werden. Bei der Teilnehmerkennung handelt es sich um ein Verkehrsdatum gem. § 96 Abs. 1 Nr. 1 TKG, so dass die weiteren Verarbeitungsvoraussetzungen für Verkehrsdaten gem. § 96 TKG zu beachten sind. Darüber hinaus sind diesbezüglich die Vorgaben des § 102 TKG zur Rufnummernanzeige und -unterdrückung zu berücksichtigen.

4.2.1.2 Private Whitelist

Bei der Anlage von Whitelists wird davon ausgegangen, dass der Teilnehmer grundsätzlich keine Kommunikation erlauben will, es sei denn, es handelt sich um gelistete Teilnehmer. Dieses Vorgehen gleicht der Nutzung elektronischer Adressbücher und dient einem ähnlichen Zweck, nämlich der sicheren Herstellung einer Kommunikationsverbindung. Gegen die Sammlung solcher Listen durch Privatpersonen ist daher nichts einzuwenden. Insbesondere für Behörden macht ein Whitelisting wenig Sinn, da Ihnen die grundsätzliche Unterdrückung der Kommunikation mit dem Bürger in aller Regel aus rechtlichen Gründen nicht möglich sein wird. Für Unternehmen könnte dies aus ökonomischen Gründen nicht in Betracht kommen. Zu beachten ist ferner, dass immer der Teilnehmer die Grundentscheidung über eine Kommunikationsunterdrückung mit Whitelistausnahme fällen sollte.

4.2.1.3 Private Blacklist

Das Blacklist-Verfahren erfordert im Gegensatz zur Whitelist zunächst keine Kommunikationsunterdrückung, sondern sieht Maßnahmen nur für gelistete Teilnehmer vor. Hier stellt sich zunächst die Frage, wie solche Listen zustande kommen und gepflegt werden, da sie für die Gelisteten ein erhebliches Diskriminierungspotenzial besitzen und daher von Dritten leicht missbraucht werden können. Einem Konzept zur Sicherung der Qualität von

Blacklist-Datenbeständen wird daher besondere Bedeutung zukommen. Darüber hinaus ist es dem Teilnehmer in der Regel freigestellt welche Kommunikationsvorgänge er annimmt und welche er ablehnt. Auch hier ist daher eine ausdrückliche Teilnehmerkontrolle notwendig. Für Behörden ergeben sich auch beim Blacklisting Einschränkungen im Hinblick auf die Gewährung rechtlichen Gehörs. Im nicht privaten oder familiären Bereich sind die Auskunfts- und Löschrchte Betroffener natürlicher Personen zu beachten, da Blacklists eine Verarbeitung personenbezogener Daten bedingen.

4.2.1.4 Statistische Blacklist

Statistische Blacklist der beschriebenen Art ergänzen das Blacklist-Konzept um eine spezifische Art der Informationsgewinnung, nämlich die statistische Auswertung von Verkehrsdaten. Diese Art der Informationsgewinnung setzt Datamining und Dataprofilung auf Basis einer statistischen Auswertung voraus. Letztere beinhaltet das Problem, dass ihr eine Fehlerquote zu eigen ist, die allenfalls minimiert, nicht aber gänzlich zu beseitigen ist. Für die genannten Vorgänge bedarf es einer datenschutzrechtlichen Rechtsgrundlage, soweit personenbezogene Daten verarbeitet werden. Darüber hinaus sind Maßnahmen zur Wahrung der Betroffenenrechte vorzusehen, um so genannten „false positives“ (zu Unrecht auf statistischen Blacklists Geführten) ihre Rechtewahrung zu ermöglichen. Im Übrigen gelten die vorherigen Anmerkungen zu Blacklists.

4.2.2 Maßnahmen

Die Identifikation von SPIT muss, um für den Teilnehmer einen Nutzen zu entfalten, in einer Maßnahme enden, die ihn von der grundsätzlichen Entgegennahme unerwünschter Werbung befreit. Solche Maßnahmen können eine Unterdrückung von Telekommunikation darstellen, wenn sie nicht explizit vom Teilnehmer veranlasst werden.

4.2.2.1 Annahme von Anrufen

Die Annahme als Maßnahme nach einer SPIT-Evaluierung stellt den Normalfall dar und ist damit grundsätzlich unproblematisch.

4.2.2.2 Ablehnung

Die gänzliche Ablehnung nach einer SPIT-Evaluierung lässt eine Kommunikation nicht zustande kommen. Sie ist damit sowohl telekommunikationsrechtlich als auch datenschutzrechtlich unter dem Gesichtspunkt einer (unzulässigen) automatisierten Einzelentscheidung zu prüfen.

4.2.2.3 Weiterleitung an dritten Anschluss

Die Weiterleitung an einen dritten Anschluss kann als unproblematisch betrachtet werden, soweit sie vom annehmenden Teilnehmer explizit so gesteuert wird, für den Anrufer keine verdeckten Mehrkosten nach sich

zieht und keine Datenschutzeinschränkungen (Sicherung der Vertraulichkeit der Kommunikation durch Netzbetreiber und Angerufenen) bedeutet.

4.2.2.4 Temporär ablehnen / Greylisting

Das Greylisting bedeutet für den Anrufer einen erhöhten finanziellen und zeitlichen Aufwand, um eine Kommunikationsverbindung herzustellen, bietet ihm jedoch letztlich die Möglichkeit dazu. Wie stark sich der Eingriff für den Anrufer darstellen wird, hängt erheblich von den Bewertungskriterien ab, die zu einem Greylisting führen sowie den Hürden für die Herstellung der Direktverbindung. In Verbindung mit einem Whitelisting kann der Aufwand auf eine Initialisierung durch das Greylisting-Verfahren beschränkt werden, wenn beide Kommunikationsteilnehmer damit einverstanden sind.

4.2.2.5 Ansage mit Hinweis auf alternativen Gesprächsaufbau

Maßnahmen des alternativen (kostenpflichtigen) Gesprächsaufbaus führen zu geringfügig höheren Kosten für den Anrufer und setzen voraus, dass dieser über eine Möglichkeit zum alternativen Gesprächsaufbau verfügt. Sollte VoIP-Telefonie die herkömmlichen PSTN-Telefonnetze gänzlich verdrängen bzw. ein Zugang zu Mehrwertnummern von einem Anschluss aus nicht möglich sein, führt diese Maßnahme zu einer faktischen Unterbindung der Kommunikation trotz grundsätzlichen Bestehens eines Kommunikationskanals.

4.2.2.6 Voicemenü

Das Voicemenü stellt nur eine kurzzeitige Behinderung des Verbindungsaufbaus dar, lässt dann aber Echtzeitkommunikation zu. Unabhängig davon werden aufgrund des längeren Telefonats möglicherweise höhere Kosten für den Anrufer entstehen. Die Effektivität für die Ausfilterung automatischer Anrufmaschinen könnte jedoch die Rückkehr zum „automatisierten Fräulein vom Amt“ für den Anrufer sinnvoll werden lassen.

4.2.2.7 Voicebox

Die Voicebox stellt eine Parallele zu heutigen Junk-Mail-Ordnern in E-Mail-Clients dar. Dies gilt insbesondere, wenn für vermeintliche SPIT-Anrufe eine eigene, von der normalen Voicebox getrennte Aufzeichnungs- und Abhörmöglichkeit eingerichtet wird. Hier besteht für den Teilnehmer die Möglichkeit, die Richtigkeit seiner Filterungsmechanismen zu überprüfen und Fehler im Nachhinein zu korrigieren. Der Zeitverzug in der Kommunikation (Aufhebung der Echtzeitkommunikation) dürfte auch telekommunikationsrechtlich nicht problematisch sein, wenn der Nutzer ihn explizit einrichtet (Vergleich mit heutigen Anrufbeantwortern, Erreichbarkeitsmanagement).

4.3 Gestaltungsoptionen

Die vorstehend geschilderten technischen Lösungsansätze sowie die darauf basierenden rechtlichen Aspekte erfordern eine Vielzahl von Entscheidungen, die einen Zuschnitt bzw. eine Konfiguration der SPIT-Abwehrlösung für konkrete Anwender bzw. Einsatzfelder sinnvoll erscheinen lassen. Einen solchen Zuschnitt sollte die SPIT-Abwehrlösung bereits durch ihr Design unterstützen. Daraus ergeben sich insbesondere die folgenden drei Anforderungen:

4.3.1 Nutzerkontrollierte Filterung

Aus verfassungs- und telekommunikationsrechtlichen wie auch aus datenschutzrechtlichen Gründen ist es geboten, die volle Kontrolle des Ob und des Wie einer Anruffilterung in die Hände des Nutzers eines Teilnehmeranschlusses zu legen. So werden rechtliche Probleme im Zusammenhang mit dem Telekommunikationsgeheimnis und datenschutzrechtliche Fragen bei der Privatnutzung einer SPIT-Abwehrlösung im Sinne des Teilnehmers und Betroffenen adressiert.. Gleichzeitig liegen die Rechte des Nutzers auf unbeobachtete Telekommunikation wie auch auf Sicherung seiner Privatsphäre in den seinen eigenen Händen.

Der Problematik der Komplexität der in diesem Projekt erarbeiteten SPIT-Abwehrlösung, die sowohl Auswirkungen auf den praktischen Gebrauchswert als auch auf die Fähigkeit zur Sicherung und Ausübung der eigenen Rechte und Interessen beeinträchtigen kann, sollte insbesondere durch die nachfolgenden nutzerunterstützenden Maßnahmen berücksichtigt werden.

4.3.2 Transparenz und Kontrolle der Datenverarbeitung und ihrer Folgen

Dem Nutzer müssen die einzelnen Maßnahmen der Identifikation, Bewertung und Behandlung von Anrufen erläutert werden. Dabei sollte er sowohl die grundsätzliche Funktionsweise als auch die verwendete Datenbasis und den Zweck der personenbezogenen Datenverarbeitungen zur Kenntnis nehmen können.

Soweit Übermittlungen personenbezogener Daten auch von Dritten aus seinem Bereich heraus erfolgen sollen, so ist auch auf den Zweck, die weitere Verwendung und die Möglichkeit zur Ausübung von Nutzerrechten hinzuweisen. Hier könnte eine zentrale Einwilligung- und Widerrufsinfrastruktur sowie eine zwingende Berücksichtigung derselben durch die SPIT-Abwehrlösung zur Sicherung und Durchsetzung von Betroffenenrechten beitragen.

Grundsätzlich sollte jede Maßnahme durch den Nutzer aktiviert werden, so dass eine Kenntnisnahme wenigstens grundlegender Prinzipien erforderlich ist und ein Mindestmaß an Kenntnisnahme gewährleistet werden kann.

4.3.3 Voreinstellungen für verschiedene Nutzergruppen

Um den Konfigurationsprozess zu erleichtern und die Nutzung in rechtmäßige Bahnen zu lenken, bietet es sich an, verschiedene Voreinstellungen für bestimmte Nutzergruppen eines Anschlusses bereitzuhalten, die bei der Ersteinrichtung der SPIT-Abwehrlösung ausgewählt werden müssen, später aber auch wieder geändert werden können.

Aufgrund der unterschiedlichen Rechtslage insbesondere für Privatnutzer, Unternehmen und Behörden erscheint das Angebot von zunächst drei Standardvoreinstellungen sinnvoll. Dabei unterscheiden sich insbesondere die Kombination der einsetzbaren Identifikations-, Bewertungs- und Behandlungsmechanismen für Anrufe. Außerdem ist in einer nutzerorientierten Dokumentation der Einstellung auf die Besonderheiten des Einsatzfeldes hinzuweisen.

5 Zusammenfassung und Ausblick

In diesem White Paper wurde dargestellt, dass SPIT-Filter künftig besondere Bedeutung für die effektive Nutzung der Internettelefonie zukommen könnte. Da sie im Vorfeld der Anrufannahme funktionieren müssen und daher nicht auf einer Analyse des Anrufinhalts beruhen können, werden die Anruferkennungen mit White- und Blacklists in einer verteilten Realisierung abgeglichen, gegebenenfalls ergänzt um eine Auswertung zusätzlicher Meta-Informationen und statistischer Analysen. Je nach Einstufung des Anrufs sind in Abhängigkeit der Nutzereinstellungen verschiedene Reaktionen möglich, zum Beispiel „Annahme“, „Abweisung“, „Umleitung auf Voicebox“, „Verweis auf kostenpflichtige Alternativtelefonnummern“ o.ä. Außerdem kann computergenerierter SPIT durch Vorschalten von interaktiven Komponenten wie einem Voicemenü ausgefiltert werden.

Einschlägige rechtliche Vorgaben aus verschiedenen Bereichen wurden betrachtet, insbesondere das Telekommunikations- und das Datenschutzrecht, aber auch das Telediensterecht, Strafrecht sowie Verwaltungsrecht. Von besonderer Bedeutung ist Transparenz und Nutzerkontrolle in Bezug auf die Realisierung der White- und Blacklists. Dies betrifft insbesondere die Möglichkeit des Imports aus anderen Quellen und der Bereitstellung der eigenen Listen für andere Nutzer.

In der vom SPIT-AL-Projekt bevorzugten Lösung werden sowohl zentrale als auch bei den einzelnen Nutzern realisierte Komponenten zum Einsatz kommen. Die in diesem White Paper diskutierten Ansätze werden im weiteren Verlauf von SPIT-AL verfeinert. Der zu implementierende Open Source-Prototyp wird über die Basisfunktionalität der rechtskonformen SPIT-Abwehrlösung verfügen. Später können weitere Features ergänzt werden.

6 Literatur

- Bundesamt für Sicherheit in der Informationstechnik:
VoIPSEC – Studie zur Sicherheit von Voice over Internet Protocol,
Oktober 2005,
<http://www.bsi.de/literat/studien/VoIP/>
- Bundesnetzagentur:
Anhörung zu Voice over IP (VoIP) – Themenweise Auswertung der
Anhörung zu Voice over IP,
Oktober 2005,
<http://www.bundesnetzagentur.de/media/archive/3173.pdf>
- Bundesnetzagentur:
Eckpunkte der regulatorischen Behandlung von Voice over IP (VoIP),
9. September 2005,
<http://www.bundesnetzagentur.de/media/archive/3186.pdf>
- Center for Democracy & Technology:
Spam 2005: Technology, Law and Policy,
Washington D.C., März 2005,
<http://www.cdt.org/speech/spam/spam2005/>
- Commission of the European Union:
Commission Staff Working Document: The treatment of Voice over
Internet Protocol (VoIP) under the EU Regulatory Framework,
14 Juni 2004,
[http://europa.eu.int/information_society/policy/ecomms/doc/info_centre/
commiss_serv_doc/406_14_voip_consult_paper_v2_1.pdf](http://europa.eu.int/information_society/policy/ecomms/doc/info_centre/commiss_serv_doc/406_14_voip_consult_paper_v2_1.pdf)
- 70. Konferenz der Datenschutzbeauftragten des Bundes und der Länder:
Entschiebung Telefonieren mit Internettechnologie (Voice over IP –
VoIP),
28. Oktober 2005,
[http://www.datenschutzzentrum.de/material/themen/presse/20051028-
dsbk-voip.htm](http://www.datenschutzzentrum.de/material/themen/presse/20051028-dsbk-voip.htm)
- Herbert Damker, Kai Rannenber, Günter Müller:
Erreichbarkeitsmanagement und mehrseitige Sicherheit aus
Benutzersicht,
Fachvorträge auf dem 4. Deutschen IT-Sicherheitskongreß des
Bundesamtes für Sicherheit in der Informationstechnik, Bonn, Mai
1995,
[http://www.wiiw.de/publikationen/Erreichbarkeitsmanagementundme.p
df](http://www.wiiw.de/publikationen/Erreichbarkeitsmanagementundme.pdf)
- Jon Peterson:
A Privacy Mechanism for the Session Initiation Protocol (SIP), RFC
3323,
November 2002,
<http://www.jdrosen.net/papers/rfc3323.txt>
- R. Pierce Reid:
Voice Spam Spam, Spamily Spam – White Paper,

Juli 2004,
http://www.qovia.com/resources/pdfs/white%20papers/qovia_spit_wpaper.doc

- Jonathan Rosenberg, Cullen Jennings, Jon Peterson:
The Session Initiation Protocol (SIP) and Spam, draft-ietf-sipping-spam-01, SIPPING Internet-Draft,
17. Juli 2005,
<http://www.ietf.org/internet-drafts/draft-ietf-sipping-spam-01.txt>
- Jonathan Rosenberg, Cullen Jennings, Jon Peterson:
Identity Privacy in the Session Initiation Protocol (SIP), draft-rosenberg-sip-identity-privacy-00, SIP Internet-Draft,
11. Juli 2005,
<http://www.ietf.org/internet-drafts/draft-rosenberg-sip-identity-privacy-00.txt>
- Stanley Milgram:
„The Small World Problem“,
Psychology Today, Mai 1967, S. 60-67