Sicherheit im Netz – Warum früher alles besser war, heute viel passiert und in Zukunft alles wieder gut wird

Erwin P. Rathgeb

Universität Duisburg-Essen
Lehrstuhl Technik der Rechnernetze

Ellernstraße 29, 45326 Essen
erwin.rathgeb@iem.uni-due.de

Zusammenfassung:

Klassische Telekommunikationsnetze, wie z. B. das Telefonnetz, waren zunächst für einen oder wenige wohldefinierte Dienste optimiert. Derzeit findet jedoch eine umfassende Entwicklung hin zu einer universellen Netzinfrastruktur auf der Basis der TCP/IP-Protokollfamilie statt. Dadurch werden – neben den unbestreitbaren Vorteilen – auch Bedrohungen und Risiken, die bisher auf das Internet beschränkt waren, zunehmend zur allgemeinen Gefahr. Die Konzepte für Angriffe und Missbrauch passen sich sehr schnell an die neuen technologischen Möglichkeiten an, wie in diesem Beitrag anhand der Internet-Telefonie (Voice over IP) verdeutlicht wird. Die derzeit praktizierte reaktive Entwicklung von Schutzmechanismen erlaubt es zwar, einen angemessen verlässlichen Netzbetrieb aufrecht zu erhalten, steigert aber die Komplexität der Systeme und Netze erheblich und führt zu Nutzungseinschränkungen und Leistungsverlusten. Deshalb sind neben diesen kurzfristigen Maßnahmen grundlegend neue Sicherheitsansätze und -architekturen notwendig. Hier bieten die Initiativen für ein von Grund auf neu konzipiertes „Future Internet“ die Chance, konsistente und umfassende Sicherheitskonzepte zu entwickeln und in der künftigen Netzarchitektur zu verankern, so dass auch langfristig tragfähige Lösungen entstehen können.

1. Einführung

Im Verlauf der letzten beiden Jahrzehnte hat sich die Art und Weise fundamental geändert, wie öffentliche Kommunikationsnetze und die von Ihnen erbrachten Dienste gestaltet und genutzt werden. Traditionell war das stark regulierte, leitungsgebundene Telefonnetz das einzige bedeutende Netz. Heute sehen wir universelle IP-basierte Netze, die zunehmend eine umfassende, gemeinsame Plattform für alle Dienste bieten – Telefonie ist nur noch einer unter vielen. Gleichzeitig ist die Mobilität ein natürlicher Aspekt unseres Kommunikationsverhaltens geworden. Auch unsere zunehmende Abhängigkeit von der durchgängigen Verfügbarkeit der vielfältigen Kommunikationsdienste – sowohl im geschäftlichen als auch im privaten Bereich – ist unbestreitbar. Die Endgeräte der Telefonie-Ära waren sehr einfach und die Dienstfunktionalität wurde weitgehend von der Netzinfrastruktur bereitgestellt. Heutige IP-basierte Netze bieten im Grunde nur eine Basis-Konnektivität, und die Dienstfunktionalität ist in die immer leistungsfähiger werdenden Endgeräte gewandert. Dies hat in kurzer Zeit zu einer nie dagewesenen Vielfalt vernetzter Anwendungen und Dienste geführt, die durch Namen wie Google, Wikipedia, Skype, YouTube, Facebook, Twitter und ähnliche repräsentiert wird. Die einfache Möglichkeit zur Einführung neuer Anwendungen hat zu einer sehr dynamischen Entwicklung geführt, die kreativen Köpfen – gutmeinenden wie bösartigen – reichlich Gelegenheiten eröffnet. Nutzungsabhängige Gebührenkonzepte für die Basiskonnektivität wurden weitgehend durch pauschale Entgelte ersetzt, und die Breitbandversorgung – bald auch drahtlos – für Privatkunden ist flächendeckend realisiert. Dadurch wurden die hauptsächlichen Hemmnisse für eine umfassende, durchgängige und globale Kommunikation für alle endlich beseitigt.

Während entscheidende Herausforderungen, wie z. B. Kapazität, Dienstgüte oder Mobilitätsunterstützung, im Laufe dieser Entwicklung weitgehend gemeistert wurden, hat sich die Situation bezüglich der Sicherheit – die in früheren Zeiten weitgehend unproblematisch war – dramatisch verschärft. Die grundlegende Kommunikations-Infrastruktur wurde während des Umbruchs auf eine offene, einheitliche und weitgehend dezentralisierte Basis migriert, die ursprünglich für vertrauenswürdige und kooperative Nutzer entwickelt wurde. Dadurch ergibt sich ganz offensichtlich ein enormes Potential für Missbrauch und Betrug. Als Konsequenz daraus sind im letzten Jahrzehnt die Angriffs- und Missbrauchsmechanismen sehr ausgeklügelt geworden, und es steht zunehmend eine finanzielle Motivation im Hintergrund.

In der Folge sollen zunächst die durch die Netzkonsolidierung auf IP-basierten Plattformen entstehenden Änderungen und Risiken kurz thematisiert werden, bevor auf den aktuellen Stand und – am Beispiel von Voice over IP – auf die weitere Entwicklung der Netzsicherheit eingegangen wird. Nach einigen Bemerkungen zur derzeitigen Vorgehensweise bei der Weiterentwicklung der Schutzmechanismen soll am Beispiel des Ansatzes aus dem G-Lab Deep Projekt exemplarisch aufgezeigt werden, wie längerfristig tragfähige, umfassende Sicherheitslösungen im Rahmen des „Future Internet“ aussehen könnten.

2. Netzarchitektur und Sicherheit

Mit der Migration der Basis-Kommunikationsinfrastruktur von den auf Telefonie als hauptsächlichen Dienst ausgerichteten klassischen Telekommunikationsnetzen (analoges Telefonnetz, ISDN) hin zu den universell nutzbaren IP-basierten Internetstrukturen hat sich in vielen Bereichen ein dramatischer Para-

ISBN 978-3-8007-3318-7

digmenwechsel vollzogen. Ermöglicht wurde dieser technische Umbruch maßgeblich durch die globale Deregulierung der Telekommunikationsmärkte, mit der ein Wettbewerbsumfeld geschaffen wurde, das schnelle und umfassende Innovationen stimuliert hat. Dabei wurden auch die Rolle und die Ausgestaltung der Standardisierung grundlegend neu definiert, so dass heute jede interessierte Organisation oder Person einfachen Zugriff auf die relevanten Dokumente hat und sogar aktiv an der Gestaltung der (Internet-)Standards partizipieren kann.

Bezüglich der Netzarchitektur haben sich paketorientierte Ansätze wegen der größeren Flexibilität und der besseren Eignung für Universalnetze (Multi-Service Networks) gegenüber kanalorientierten (durchschaltevermittelten) Lösungen durchgesetzt. Beim Netzbetrieb hat die dynamische Selbstkonfiguration des Netzes und seiner Komponenten die strikte Detailadministration weitgehend verdrängt. Dadurch ergeben sich Vorteile bei der Flexibilität und Einsparpotentiale beim Netzbetrieb, eine übergeordnete Kontrolle und Überwachung – auch von unerwünschten Aktivitäten – wird aber erheblich erschwert.

In den klassischen Netzen konnten Aktivitäten eindeutig einem Anschluss, und damit einem Teilnehmer, zugeordnet werden (Trust by Wire). Auch bei den zellularen Mobilfunknetzen ist dies durch die SIM-Karten möglich, die eindeutig einem Teilnehmer zugeordnet sind. Im heutigen Internet ist eine solche Zuordnung – auch wegen der dynamischen Konfiguration und der zunehmenden Mobilität der Teilnehmer – nur noch sehr bedingt möglich. Da der Sender alle abgeschickten Informationen, insbesondere auch die Adressinformationen, uneingeschränkt manipulieren kann, können Angreifer weitgehend anonym bleiben.

Bei den verwendeten Kommunikationsprotokollen hat sich eine Vielzahl von Möglichkeiten und Optionen ergeben, die täglich größer wird. Dabei haben sich allerdings in der Praxis Basisprotokolle etabliert, die intensiv und durchgängig genutzt werden. Die sehr spezifischen und meist komplexen Protokolle und Schnittstellen der klassischen Netze wurden durch offene, universell anwendbare ersetzt. Dabei wurde auch die beim ISDN strikt umgesetzte Trennung von Nutz- und Steuerdaten in vielen Bereichen wieder aufgehoben. Durch die durchgängige und oftmals dienstübergreifende Nutzung einheitlicher und offener Basisprotokolle für die Steuerung der Netze und der Dienste eröffnen sich den Angreifern im Internet umfassende und leicht zu handhabende Möglichkeiten zur Manipulation.

Ein weiterer Umbruch hat sich in der Art vollzogen, wie „Dienste“ in den Netzen angeboten werden. In den klassischen Kommunikationsnetzen wurden wenige, sehr wohldefinierte und großteils standardisierte Dienste von den Netzbetreibern angeboten. Die hierfür erforderliche Dienstlogik wurde dabei weitgehend in den Netzknoten realisiert, während die Endgeräte relativ einfach gehalten waren. IP-basierte Netze hingegen bieten hauptsächlich eine grundlegende Konnektivität, während die Dienstlogik in den Endgeräten angesiedelt ist. Damit kann sie weitestgehend von den Nutzern selbst realisiert und bestimmt werden. Dies hat zu einer enormen Dynamik und Vielfalt an Diensten und Anwendungen geführt, macht aber auch die Kontrolle und Verhinderung von Angriffen, Betrug und Dienstmissbrauch sehr viel schwieriger und aufwändiger.

Unter dem Begriff „Next Generation Network“ (NGN) wurden bei ITU-T und ETSI entsprechende Standardisierungsaktivitäten im Festnetzbereich durchgeführt, im Bereich der Mobilfunknetze zielen die Planungen ebenfalls auf ein „All-IP“-Netz, das den nächsten Entwicklungsschritt nach UMTS darstellen soll. Auch über die klassische Kommunikation hinaus werden IP-basierte Ansätze in vielen Bereichen Einzug halten, ob im Rahmen von „Smart Grid“ für die flexible Steuerung künftiger Energienetze, im Rahmen der E-Health-Initiativen im Gesundheitsbereich oder als Ersatz für die unterschiedlichen Bussysteme in Fahrzeugen (IP in the Car).

All diese Ansätze versprechen den Betreibern organisatorische, betriebliche und ökonomische Vorteile. Auch für die Nutzer ergibt sich eine Reihe potenzieller Vorteile durch flexible, kostengünstige und bedarfsgerechte Nutzungsmöglichkeiten. Allerdings führt die Konvergenz der Netze auch dazu, dass die in den einzelnen Netzen – und insbesondere in den IP-basierten – existierenden Angriffs- und Missbrauchsmöglichkeiten durch die Verwendung einer einheitlichen Plattform auch zur Bedrohung in den bisher durch spezifische, eigenständige Netzarchitekturen geschützten Bereichen werden.

Im folgenden Abschnitt soll dies anhand des Telefoniedienstes dargestellt und erläutert werden.

3. Stand der Bedrohungen und ihre Weiterentwicklung

Flächendeckende Untersuchungen von Softwareherstellern zur Entwicklung und Verbreitung von Schadsoftware, deren Ergebnisse regelmäßig veröffentlicht werden (z. B. [1,2]) zeigen, dass an das Internet angeschlossene Rechner permanent automatisierten Angriffen ausgesetzt sind. Eigene Langzeituntersuchungen [3] mit speziell für diesen Zweck eingerichteten Ködernetzen haben diese Aussagen eindeutig bestätigt. Die im Ködernetz vorhandenen Rechner wurden schon unmittelbar nach ihrer Aktivierung entdeckt obwohl sie keinerlei Aktivitäten im Internet ausführten und auch nicht, z. B. über das Domain Name System (DNS), explizit im Netz bekannt gemacht wurden. In der Folge waren sie permanent Angriffen aus dem Netz ausgesetzt, wie der in Abbildung 1 dargestellte Ausschnitt aus den Messprotokollen zeigt. Alarme (Alarms) bezeichnen dabei die Angriffe, die explizit einer spezifischen Schadsoftware zugeordnet werden konnten, Warnungen (Warnings) bezeichnen Hinweise auf verdächtige Aktivitäten, die jedoch nicht explizit zugeordnet werden konnten.

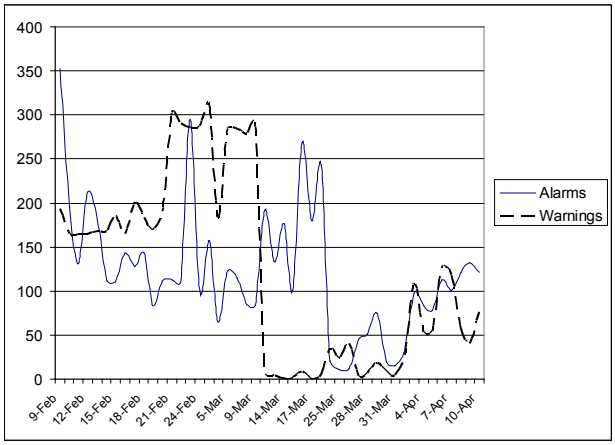

Abb. 1: Typische Messwerte für Angriffe aus dem Internet

Ziel der Angriffe ist es typischerweise, einen nicht autorisierten, privilegierten Zugriff auf den Rechner zu erlangen und die Kontrolle über diesen zu übernehmen. Bei einer über mehrere Wochen gezielt beobachteten erfolgreichen Übernahme [4] nahm der Rechner Kontakt zu einem Server im Internet auf und wurde in ein sogenanntes „Botnet“ eingegliedert, über das ein Angreifer eine Vielzahl übernommener Rechner kontrollieren und koordiniert steuern kann. Nachdem über einen längeren Zeitraum mehrere Nutzer des Botnets den Rechner genau untersucht hatten, wurde ein „SPAM-Proxy“ installiert, der

ISBN 978-3-8007-3318-7

nach seiner Aktivierung in kurzer Zeit versuchte, mehrere tausend SPAM-Emails zu verschicken.

Bei der Weiterentwicklung der Schadsoftware (Malware) hat sich in den letzten Jahren ein klarer Trend zur Professionalisierung gezeigt. Ziel der Aktivitäten sind zunehmend finanziell motivierte Betrugsaktivitäten. Dies äußert sich z. B. darin, dass ein überwiegender Anteil der SPAM-Mails inzwischen sogenannte „Phishing"-Nachrichten enthält, mit denen Zugangsinformationen zu Konten und Nutzer-Accounts erschlichen werden sollen.

Als Konsequenz aus dieser allgegenwärtigen Bedrohungssituation haben die Softwarehersteller ihre Bemühungen zur Vermeidung und Behebung von Schwachstellen intensiviert. Die regelmäßige Suche nach Sicherheitsupdates, Malware-Scanner und SPAM-Filter sind inzwischen in die Betriebssysteme und Anwendungen integriert, und können problemlos auch von Nutzern ohne Spezialwissen sinnvoll angewendet werden. Dadurch hat sich trotz der andauernden Angriffsaktivitäten eine Situation ergeben, in der bei Beachtung einiger grundlegender Verhaltensregeln ein hinreichend sicherer Zugang zum Internet für den Privatnutzer gegeben ist.

Allerdings ist zu beobachten, dass nahezu zeitgleich mit neuen Technologien und Anwendungen auch entsprechende Bedrohungs- und Angriffsmuster entwickelt werden. So sind z. B. mit Einführung der Smartphones, die es den Nutzern erlauben zusätzliche Softwareanwendungen zu installieren, in signifikantem Umfang spezielle Schadsoftwarevarianten für diese Geräte aufgetaucht [5].

Eine Analyse der Bedrohungssituation für verschiedene Technologien und Anwendungen zeigt, dass es eine Reihe von Kriterien gibt, die diese besonders attraktiv für Angreifer machen. Die flächendeckende Verwendung einheitlicher, offener und flexibler Protokolle liefert ein klar definiertes Angriffsziel und verspricht einen hohen Nutzen in Relation zu dem Aufwand, der für die Entwicklung der Angriffswerkzeuge investiert werden muss. Dienste und Anwendungen, die weltweit genutzt werden und eine hohe Durchdringung der Nutzerpopulation aufweisen, generieren einen großen Pool potenzieller Angriffsziele. Damit ergibt sich auch eine ausreichende Erfolgswahrscheinlichkeit für relativ simpel angelegte Angriffe und Betrugsversuche – wie das Beispiel von SPAM und Phishing eindrucksvoll zeigt. Außerdem muss ein hohes Nutzen/Kostenverhältnis für die Angriffe gegeben sein. Dieses entsteht entweder dadurch, dass die Kosten vernachlässigbar gering sind (siehe SPAM) oder dadurch, dass ein erfolgreicher Angriff einen signifikanten finanziellen Vorteil erbringt.

Alle diese Risikofaktoren sind bei einer Migration des Telefoniedienstes von den klassischen Telefonnetzen auf eine IP-basierte Basis (Voice over IP, VoIP) gegeben: Als einheitliches Basisprotokoll für VoIP – und für weitere Multimediadienste – hat sich das SIP-Protokoll [6] weltweit etabliert. Die Netzbetreiber stellen zunehmend ihre Telefonieangebote auf VoIP um, so dass die Marktpenetration schnell zunimmt. Die Kosten für „normale" VoIP-Telefonate sind oftmals mit den Pauschalpreisen für den Internetzugang abgedeckt, so dass sie praktisch kostenfrei sind. Andererseits werden für spezielle Verbindungen (Auslandsgespräche, Anrufe zu 0900-Nummern) erhebliche Gebühren pro Verbindung erhoben.

Gemäß der oben beschriebenen Kriterien kann also vermutet werden, dass der VoIP-Dienst für Angreifer äußerst attraktiv ist und zeitnah entsprechende Angriffsszenarien entwickelt werden. Im nächsten Abschnitt soll deshalb anhand von aktuellen Untersuchungen überprüft werden, ob dies auch in der Realität der Fall ist.

4. Existieren schon VoIP-spezifische Bedrohungen?

Der prinzipielle Ablauf bei der VoIP-Kommunikation ist wie folgt: Der Nutzer verfügt über eine (alphanumerische) Kennung, die in Verbindung mit einem bestimmten SIP-Provider eindeutig ist, z. B. user4711@provider-x.de. Er registriert sich mit seiner Kennung bei einem SIP-Server seines Providers, so dass dort die Zuordnung seiner SIP-Kennung zu seiner momentanen IP-Adresse bekannt ist. Die Anmeldung kann dabei von überall her über das Internet erfolgen. Durch die so hergestellte Zuordnung ist der Nutzer dann für ankommende Gesprächsanfragen auffindbar. Abgehende Verbindungsanfragen schickt der Nutzer dann an seinen SIP-Server, der diese entsprechend weiterleitet. Die eigentlichen Sprachdaten werden dann, je nach Anwendungsszenario, direkt zwischen den Teilnehmern oder unter Einbeziehung des SIP-Servers (Proxy) über das Internet ausgetauscht. Deshalb werden VoIP-Gespräche in der Regel nicht extra in Rechnung gestellt und sind durch die Gebühren des Internetzugangs mit abgedeckt. Der SIP-Provider stellt typischerweise auch Netzübergänge zu den klassischen Sprachnetzen her, so dass ein SIP-Teilnehmer auf diesem Weg alle Telefonteilnehmer weltweit erreichen kann. Die dabei entstehenden Kosten werden dem Nutzer über das zur Kennung gehörige Nutzerkonto in Rechnung gestellt.

Aus diesem Nutzungsszenario ergeben sich unterschiedliche dienstspezifische Angriffs- und Missbrauchsmöglichkeiten, die in klassischen Telefonnetzen unbekannt waren. Diese stellen gezielte Anpassungen im Internetumfeld bekannter Szenarien an die neue VoIP-Technologie dar. Zunächst besteht die Möglichkeit, weitgehend kostenfrei VoIP-Telefonate zu führen. Dies ist für das Telemarketing sehr interessant, bietet aber auch die Möglichkeit, mit sehr geringem Kostenaufwand massenhafte, meist automatisierte Werbeanrufe zu generieren. Man spricht in diesem Zusammenhang von SPIT (SPAM over Internet Telephony), da hier die gleichen Mechanismen wie beim E-Mail-SPAM greifen. Im Extremfall können auch Teilnehmer oder ganze Telefonanlagen durch solche Gespräche blockiert werden (Denial of Service).

Ein SIP-Nutzer kann sich von überall her bei seinem Provider anmelden und über diesen kostenpflichtige Gespräche in andere Netze führen. Deshalb kann auch ein Angreifer versuchen, sich unter einer falschen Kennung anzumelden (Registration Hijacking), um dann unerlaubt über ein fremdes Nutzerkonto gebührenpflichtige Gespräche zu führen (Toll Fraud).

Um nachzuweisen ob diese Bedrohungen schon real sind, wurde am Lehrstuhl ein speziell auf VoIP ausgerichtetes Ködernetz (VoIP Honeypot) entwickelt und aufgebaut, bei dem ein modifizierter Asterisk [7] SIP-Server als Angriffsziel und Protokollierungseinheit eingesetzt wird. Eine vorgeschaltete Honeywall [8] erlaubt darüber hinaus die Aufzeichnung aller Datenpakete der Angriffe. In einer seit 2008 laufenden Untersuchung wurde das VoIP Honeypot System ohne weitere Aktivitäten zur Bekanntmachung – wie bei der Ködernetz-Untersuchung bezüglich allgemeiner Malware – nach der Aktivierung von den Angreifern gefunden. Wie die Übersichtsstatistik in Abbildung 2 zeigt, erfolgen die spezifischen Angriffe zwar noch mit einer (im Vergleich zu allgemeinen Malware-Attacken) relativ geringen Intensität, allerdings wird auch der VoIP Honeypot kontinuierlich attackiert.

ISBN 978-3-8007-3318-7

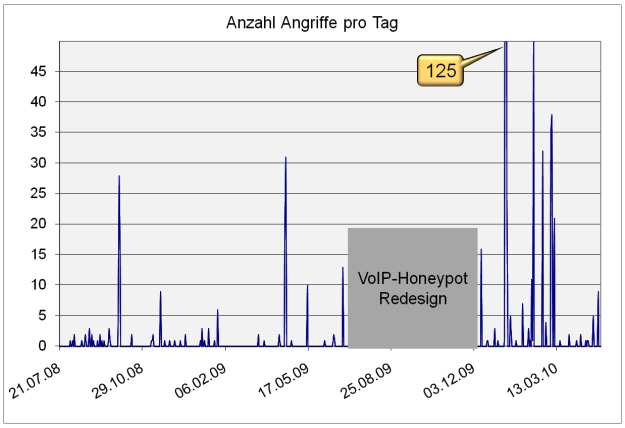

Abb. 2: Übersicht über die Messungen mit dem VoIP Honeypot

Die Auswertung der Daten ergibt zwar auch Hinweise auf SPIT-Aktivitäten, aber in der Mehrzahl handelt es sich bei den Aktivitäten um Registration Hijacking und Toll Fraud Versuche in unterschiedlichen Varianten. Bei den Versuchen zum Registration Hijacking werden, teilweise sehr systematisch, die an dem SIP-Server eingerichteten Accounts gescannt. In der Folge werden dann teilweise massive Wörterbuch-Attacken gestartet, um die entsprechenden Anmeldepasswörter herauszufinden. Bei anderen Angriffsvarianten werden direkt Verbindungsanfragen an den Server gestellt, mit denen ausländische Anschlüsse bzw. gebührenpflichtige Sondernummern (0900-Nummern) im In- und Ausland erreicht werden sollen.

Die Angriffe haben ihren Ursprung im Prinzip weltweit, so dass die Situation durchaus mit der generellen Malware-Situation vergleichbar ist – auch wenn die Intensität derzeit noch geringer ist. Ähnlich wie für allgemeine Malware sind schon Softwarewerkzeuge frei im Internet verfügbar, mit denen die beschriebenen Angriffe ohne spezielle Fachkenntnisse durchgeführt und mit angemessenem Aufwand auch komplett automatisiert werden können [9].

5. Was wird bisher getan?

Die TCP/IP-Architektur und ihre Protokolle waren ursprünglich auf ein kooperatives Nutzerumfeld ausgerichtet, so dass durchgängige Sicherheitsmaßnahmen nicht vorhanden waren. Im Lauf der Zeit wurden diese schritthaltend „nachgerüstet“, um aktuell auftretende Probleme zu lösen. Dies geschah einerseits durch kryptographische Erweiterungen für die Protokolle selbst, andererseits durch die Definition spezieller Zusatzprotokolle zur Absicherung der Kommunikation, wie z. B. IPSec oder TLS (Transport Layer Security). Diese Protokolle können in den verwendeten Protokollstack eingebunden werden und stellen kryptographische Sicherungsfunktionen auf den unterschiedlichen Schichten zur Verfügung. Eine weitere Maßnahme sind Zusatzkomponenten wie Malware-Scanner, Firewalls, Intrusion Detection Systeme u. ä., die Systeme oder Netzbereiche schützen sollen. Diese Maßnahmen zielen zunächst auf die Absicherung gegen generelle Angriffe, allerdings werden auch spezifische Mechanismen bzw. Funktionen zum Schutz spezieller Anwendungen entwickelt. Beispiele hier sind SPAM-Filter für den E-Mailverkehr oder SPIT-Filter, die eine entsprechende Funktion bei unerwünschten Werbeanrufen übernehmen.

Dieses Vorgehen dämmt zwar die bestehenden Probleme soweit ein, dass eine angemessene Nutzung der Netze, Dienste und Anwendungen möglich ist. Um überhaupt funktionierende Sicherheitslösungen realisieren zu können, müssen allerdings auch Grundprinzipien der Netzarchitektur, z. B. die konsequente Funktionstrennung zwischen den Protokollschichten, teilweise aufgegeben werden. Diese reaktive Vorgehensweise bei der Weiterentwicklung der Protokolle ist nicht nur im Sicherheitsbereich zu beobachten, auch in anderen kritischen Bereichen, wie z. B. Dienstgüte oder Mobilitätsunterstützung, wird entsprechend verfahren. Insgesamt erhöht sich dadurch die Komplexität der Netz- und Protokollarchitektur beträchtlich, was zu funktionalen Einschränkungen und auch zu einer signifikant verminderten Leistungsfähigkeit führt.

Durch die enorm steigende Nutzerzahl, die Konsolidierung aller Netze auf einer IP-Basisinfrastruktur, die Vielfalt neuer Anwendungen und die zunehmende Abhängigkeit von den Kommunikationsnetzen steigen gleichzeitig die Anforderungen an die Netze erheblich an. Deshalb warnen manche Experten seit einigen Jahren vor einem bevorstehenden Kollaps des Internets und fordern eine grundlegende Erneuerung der Internetarchitektur. Diese Erneuerung soll unabhängig von den beschränkenden Randbedingungen der vorhandenen TCP/IP-Architektur konzipiert werden. Dies geht soweit, dass auch disruptive „Greenfield“-Ansätze verfolgt werden sollen, bei denen alle Paradigmen bis hin zur Verwendung geschichteter Protokollarchitekturen zur Disposition gestellt werden. Diese Ideen haben weltweit zu massiven Forschungsinitiativen unter dem Begriff „Future Internet“ geführt. In Deutschland konzentrieren sich diese Forschungen auf die G-Lab Initiative (www.german-lab.de), bei der in einer Vielzahl von Einzelprojekten unterschiedliche Aspekte und Lösungsansätze für das Future Internet untersucht werden. Für die praktische Erprobung wurde in diesem Zusammenhang auch eine deutschlandweite Experimental-Plattform gebaut.

Die Überlegungen zum Future Internet eröffnen auch die Chance, sich mit umfassenden Lösungen für die Sicherheitsproblematik zu befassen, die als einer der kritischsten Punkte der aktuellen Internetarchitektur identifiziert wurde. Im folgenden Abschnitt sollen kurz einige Ansätze beispielhaft vorgestellt werden, die wir im Rahmen des G-Lab Deep Projekts (www.g-lab-deep.de) mit unseren Partnern verfolgen.

6. Neue Ansätze für das Future Internet

Im G-Lab Deep Projekt wird ein neuartiger, serviceorientierter Netzwerkansatz verfolgt [10]. Dienste sollen dabei nicht fest vordefiniert, sondern durch funktionale Komposition dynamisch aus Basiskomponenten orchestriert werden.

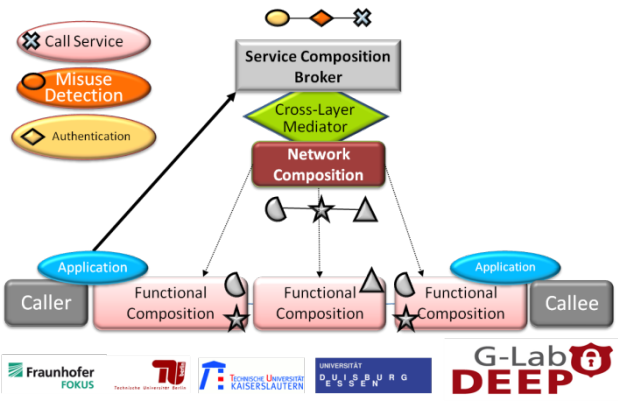

Abb. 3: Der G-Lab Deep Ansatz

Dieser aus der Softwareentwicklung bekannte Ansatz soll dabei nicht nur auf die Dienstschicht angewendet, sondern

ISBN 978-3-8007-3318-7

auch auf das Netz selbst übertragen werden. Durch dieses in Abbildung 3 schematisch dargestellte Konzept sollen einerseits Dienste flexibel und bedarfsgerecht verfügbar gemacht und andererseits die Netzressourcen optimal an deren Bedürfnisse angepasst werden.

Ein Schwerpunkt der Arbeiten liegt dabei auf einem Konzept, bei dem spezifische Erkennungs- und Schutzfunktionen bei Bedarf dynamisch in die Dienstlogik integriert werden können. Diese sollen über das Netz Informationen austauschen, um mit entsprechenden Mechanismen im Netz zu kooperieren und zu interagieren wie in Abbildung 4 angedeutet.

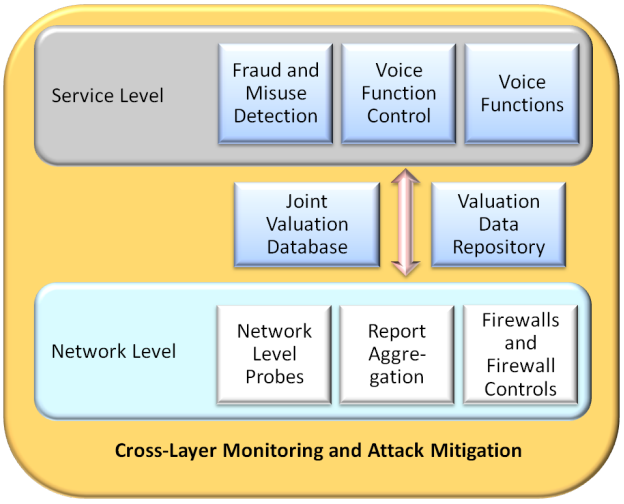

Abb. 4: Schichtenübergreifende Kooperation zur Erkennung und Abwehr von Angriffen

Als Anwendungsszenario wird in dem Projekt ein Telefoniedienst betrachtet [11]. Missbrauchssensoren, z. B. für SPIT, Registration Hijacking und Toll Fraud können bei Bedarf dynamisch in die Prozesskette der Kommunikation eingefügt werden. Sie stellen sehr detaillierte, aber nur lokal relevante Informationen über unerwünschte Aktivitäten zur Verfügung. Diese Informationen von unterschiedlichen Teilnehmern werden von einer Überwachungskomponente im Netz gesammelt, konsolidiert und ausgewertet, um einen Überblick über den Gesamtzustand und die Signifikanz der Anomalien zu erhalten. Als Reaktion können den Teilnehmern Konfigurationsinformationen für Abwehrkomponenten, z. B. SPIT-Filter, verfügbar gemacht werden, so dass auch bisher nicht direkt betroffene Teilnehmer proaktiv geschützt werden können.

Gleichzeitig können entsprechende Überwachungsmaßnahmen auf der Netzebene angestoßen und parametrisiert werden, um flächendeckend die verdächtigen Aktivitäten zu beobachten und zu analysieren. Durch die in der Netzinfrastruktur vorhandenen Möglichkeiten können auch die Quellen des unerwünschten Verkehrs lokalisiert und die Angreifer, z. B. durch gezielte Filterung, neutralisiert werden. Durch solche und ähnliche Ansätze können durchgängige, über Dienste und Netzinfrastrukturen hinweg konsistente Schutzmechanismen von Anfang an in die neue Architektur integriert werden und so zu langfristig tragfähigen Lösungen führen.

Zusammenfassung

Durch die Netzkonsolidierung auf Basis einer TCP/IP-basierten Basisinfrastruktur ergeben sich für Netzbetreiber und Nutzer erhebliche Vorteile bezüglich Funktionalität und Kosten. Durch die Aufgabe der Netzvielfalt sowie der strengen Administration und Kontrolle zugunsten von mehr Effizienz und Flexibilität werden aber auch die Risiko- und Bedrohungspotenziale aus den einzelnen Bereichen zu einer allgemeinen Gefahr.

Die Angriffs- und Missbrauchskonzepte zielen zunehmend auf finanzielle Vorteile ab, so dass die hierfür verwendeten Angriffswerkzeuge unter durchaus professionellen Randbedingungen weiterentwickelt werden. Dies führt dazu, dass sich die Angriffe und Missbrauchskonzepte sehr rasch an neue technologische Möglichkeiten anpassen und diese nutzen.

Bei der Entwicklung von Gegenmaßnahmen wurden die Anstrengungen allerdings ebenfalls erheblich intensiviert. Dies, und vor allem die wachsende Sensibilisierung der Nutzer für Sicherheitsprobleme und deren Lösungen führt dazu, dass trotz der allgegenwärtigen Bedrohung in der Regel eine hinreichend verlässliche Kommunikation gewährleistet werden kann.

Allerdings führen diese Anstrengungen auch zu einer zunehmenden Komplexität der Systeme und Netze, so dass sie lediglich als kurzfristige Lösungen akzeptabel sind. Durch die Initiativen im Zusammenhang mit dem „Future Internet“, bei denen die Sicherheitsproblematik als eines der Schlüsselthemen identifiziert wurde, besteht nun erstmals auch die Chance konsistente, in die Basisarchitektur integrierte Sicherheitskonzepte zu entwickeln, die zu langfristig tragfähigen Lösungen führen werden.

ISBN 978-3-8007-3318-7

7. Referenzen

[1] Sophos, „Security Threat Report: 2010“, http://www.sophos.com/sophos/docs/eng/papers/sophos-security-threat-report-jan-2010-wpna.pdf, abgerufen am 08.11.2010.

[2] Symantec, „Symantec Global Internet Security Threat Report – Trends for 2009” Volume XV, April 2010, http://eval.symantec.com/mktginfo/enterprise/white_papers/b-whitepaper_internet_security_threat_report_xv_ 04-2010.en-us.pdf, abgerufen am 08.11.2010.

[3] Riebach, S.; Rathgeb, E.P.; Toedtmann, B., „Efficient Deployment of Honeynets for Statistical and Forensic Analysis of Attacks from the Internet”, in: Proceedings of "IFIP NETWORKING 2005". Waterloo Ontario, Canada (2005).

[4] Riebach, S.; Rathgeb, E.P.; Toedtmann, B., „Risk Assessment of Production Networks Using Honeynets – Some Practical Experience”, in: Proceedings of „The First Information Security Practice and Experience Conference (ISPEC 2005)”, Singapore (2005).

[5] Gostev, A.; Maslennikov, D., „Mobile Malware Evolution: An Overview, Part 3”, http://www.securelist.com/en/analysis/204792080/ Mobile_Malware_E, 29.10.2009, abgerufen am 08.11.2010.

[6] Trick, U.; Weber, F., „SIP, TCP/IP und Telekommunikationsnetze”, Oldenbourg; 3. überarbeitete und erweiterte Auflage, 7. Mai 2007, ISBN 3486582283.

[7] Asterisk, „Open Source Communications“, http://www.asterisk.org/, abgerufen am 08.11.2010.

[8] The Honeynet Project, „The Honeywall project site”, https://projects.honeynet.org/honeywall/, abgerufen am 08.11.2010.

[9] Knaup, P., „Konzept und Realisierung dienstspezifischer Angriffsszenarien für eine Future Internet Plattform”, Bachelorarbeit im Studiengang Angewandte Informatik – Systems Engineering, ICB, Universität Duisburg-Essen, 30.05.2010.

[10] Becke, M. et.al., „A Demonstrator for Cross-Layer Composition”, in: Proceedings of Euroview 2010, Würzburg, August 2010.

[11] Becke, M. et.al., „Addressing Security in a Cross-Layer Composition Architecture”, in: Proceedings of Euroview 2010, Würzburg, August 2010.

Prof. Dr.-Ing. Erwin P. Rathgeb

Universität Duisburg-Essen

Institut für Experimentelle Mathematik

Alfried Krupp von Bohlen und Halbach-Lehrstuhl
Technik der Rechnernetze

Ellernstraße 29

45326 Essen

Erwin P. Rathgeb wurde 1958 in Ulm geboren. Er erhielt 1985 das Diplom und 1991 den Doktorgrad in Elektrotechnik von der Universität Stuttgart. Er war von 1985 bis 1990 Mitarbeiter am IKR der Universität Stuttgart (Professor Paul J. Kühn) wo er auch eine Forschungsgruppe zum Thema verteilte Systeme leitete.

Nach einem einjährigen Forschungsaufenthalt bei Bellcore, New Jersey, arbeitete er zunächst bei Bosch Telekom in Backnang und dann von 1993 bis 1999 bei Siemens in München. In unterschiedlichen Positionen trug er zur Entwicklung von Konzepten für kommerzielle ATM-Vermittlungsstellen und ATM-basierte Multiservicenetze bei.

Seit 1999 ist er Inhaber des Alfried Krupp von Bohlen und Halbach-Stiftungslehrstuhls „Technik der Rechnernetze“ am Institut für Experimentelle Mathematik der Universität Duisburg-Essen.

Professor Rathgeb ist Senior Member bei IEEE und Mitglied bei IFIP, GI und ITG. Er ist Autor eines bei Springer erschienenen Buchs über ATM und hat zahlreiche Artikel in Fachzeitschriften und auf internationalen Fachtagungen veröffentlicht.

Einer seiner Forschungsschwerpunkte ist die Netzsicherheit, mit der er sich seit 1999 beschäftigt. Seine Beiträge zu Ende-zu-Ende Sicherheitslösungen für SCTP führten zu zwei Internetstandards. Weitere Forschungsergebnisse umfassen neuartige Filterkonzepte zum Schutz von großen Netzen und die Nutzbarmachung von Ködernetzkonzepten für die Erkennung dienstspezifischer Angriffe. In aktuellen Projekten befasst er sich mit der Sicherheit der Internet-basierten Telefonie (Voice over IP) und von Peer-to-Peer-Netzen. Im Rahmen der deutschen „Future Internet“-Initiative G-Lab forscht er derzeit an schichtenübergreifenden Sicherheitskonzepten für ein neues, dienstorientiertes Internet.

Seit 2005 organisiert und veranstaltet Professor Rathgeb regelmäßig und erfolgreich den „Essener Workshop zu neuen Herausforderungen in der Netzsicherheit“, der ein Forum für Sicherheitsexperten aus Wissenschaft und Industrie bietet. 2006 initiierte er die ITG-Fachgruppe 5.2.2 „Sicherheit in Netzen“ deren Leiter er seitdem ist.

ISBN 978-3-8007-3318-7