Security for Future Services
in Next Generation Networks

von

Professor Dr. Norbert Pohlmann

Leiter des Instituts für Internet-Sicherheit
und Professor im Fachbereich Informatik
an der Fachhochschule Gelsenkirchen

Inhaltsverzeichnis

1 Ausgangspunkt
2 Wie sehen Netze heute aus?
3 Zukünftige Netze (NGNs)
4 Sicherheitsanforderungen
5 Identity Management
6 E-Mail-Verlässlichkeit
7 Web Service Security
8 Gemeinsame Sicherheitsinfrastruktur
9 Gefahren der Zukunft?
10 Wie sicher ist „sicher"?
11 Eine Frage der Vertrauenswürdigkeit
12 Wer hat die Macht?
13 Fazit
14 Literatur
15 Verfasserportrait

Abkürzungen

NGN	Next Generation Network(s)
NGS	Next Generation Service(s)
QoS	Quality of Service
PSTN	Public Switched Telephone Network(s)
IN	Intelligent Network(s)
AAA	Authentication, Autorization, Accounting
XKMS	XML Key Management Specification
PKI	Public Key Infrastructure
SSL	Secure Socket Layer
CA	Certification Authority

1 Ausgangspunkt

Computer, das Internet und weitere Netzdienste haben unseren Alltag verändert. Wir entwickeln uns zunehmend zu einer vernetzten Wissens- und Informationsgesellschaft, in der Verlässlichkeit und Vertrauenswürdigkeit von Informations- und Kommunikationstechnik mit ihren Diensten eine besondere Rolle spielt. Das Internet und weiter Netzdienste (z.B. GSM, UMST) sind in den letzten Jahren rasant gewachsen und bieten mit der eigenen IT-Infrastruktur vielfältige Möglichkeiten.

Im Wirtschaftsleben ist zu beobachten, dass immer mehr Geschäftsprozesse mithilfe von IT-Systemen über das Internet abgewickelt werden. Elektronische Marktplätze und standortübergreifende Informationsverarbeitung sind dabei wichtige Beispiele. Das Web, die E-Mail-Kommunikation, mobile Dienste haben z.B. enorme Vorteile gebracht und es besteht in Zukunft noch ein sehr großes Potential, einerseits Geschäftsprozesse rationaler abzuwickeln und gleichzeitig neue Geschäftsfelder zu ermöglichen.

Aber mit den Chancen steigen auch die Risiken – und mit ihnen auch die Notwendigkeit, angemessene IT-Sicherheitsmaßnahmen anzuwenden, damit in der „elektronischen Welt" eine Basis der Vertrauenswürdigkeit bestehen kann.

Die herkömmlichen Geschäftprozesse in der „realen Welt" wurden und werden durch Sicherheitssysteme wie Pförtner, Safes oder Sicherheitstransporter geschützt. Auch wenn diese Mechanismen keine hundertprozentige Sicherheit gewährleisten können, so können mit ihrer Hilfe doch Risiken wirksam begrenzt werden. Solche – oder äquivalente Sicherheitsmechanismen benötigen wir auch in der elektronischen Welt.

Das gilt umso mehr, wenn wir den immer weiter steigenden Wert elektronischer Informationen in Betracht ziehen. Informationen, die auf Rechnersystemen gespeichert oder durch Netze übertragen werden, stellen nicht selten erhebliche finanzielle Werte dar. Kundendaten, Entwicklungsunterlagen, Strategiekonzepte oder Logistikinformationen können nicht nur persönlich empfindlich sein, sondern auch Bereiche wie den Börsenmarkt direkt und nachhaltig beeinflussen. Solche Bits und Bytes können schnell mehrere Millionen Euro wert sein. Aber auch die elektronischen Prozesse selbst stellen einen nicht zu unterschätzenden Wert dar.

Umso wichtiger wird es sein, die Herausforderung zu meistern, für eine nachhaltige und passende Vertrauenswürdigkeit von Informations- und Kommunikationstechnik zu sorgen.
Dies ist notwendig, damit wir einerseits die schon genutzten Dienste weiterhin verlässlich nutzen können und andererseits, mit Vertrauenswürdigkeit als Enabler, eine breite Basis für weitere neue Dienste schaffen und erhalten können.
Während es heute Sicherheitslösungen gibt, die auf die jeweilige Technologie oder ein spezielles Angebot zugeschnitten sind, wird es in Zukunft wichtig sein, all diese Technologien zu einem Next Generation Network zu verschmelzen.
Das Zusammenwachsen dieser verschiedenen Technologien und Angebote bedeutet, dass die Sicherheit in den neuen Dienstleistungen, mit neuen Übergängen zwischen Verantwortung und komplexen Beziehungen kontrolliert werden muss. In offenen Systemen brauchen wir andere, betreiberübergreifende Lösungskonzepte für funktionierende Sicherheitsmechanismen.
Der Artikel zeigt die neuen Anforderungen an ein NGN auf, und macht Vorschläge für Strategien und Lösungen mit dem Ziel, einen sicheren und vertrauenswürdigen Betrieb von Informations- und Kommunikationstechnik zu schaffen und nachhaltig zu sichern.

2 Wie sehen Netze heute aus?

In den bestehenden Public Switched Telephone Networks (PSTN) – analog, ISDN und Mobilfunk - werden Mehrwertdienste wie Voice-Mail, Free-Call, 0800- oder 0180-Nummern meist über Intelligent Networks (IN) abgebildet.
Dieses Verfahren ist aufgrund der Systemkosten und dem hohen Administrationsaufwand sehr kostenintensiv und bleibt damit ausschließlich den Netzbetreibern vorbehalten. Die heutigen Netz- und Service-Betreiber (Festnetz, Mobilfunk, aber auch "alternative" Betreiber und Provider) müssen deshalb verstärkt neue Services und Applikationen zusätzlich zu ihren (Netz-) Diensten anbieten.

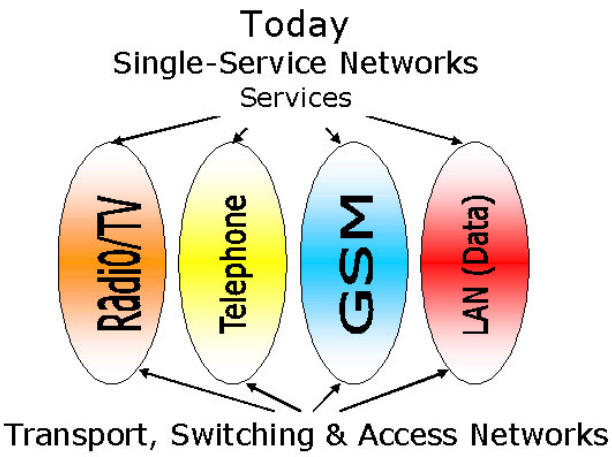

Abb. 1: Heutige Single Service Networks

Services und Applikationen auf quasi fremde Netze zu adaptieren würde den Spielraum für die Anbieter deutlich erweitern.

Mit diesen Möglichkeiten wären weitere bzw. neue Mehrwertdienste für die Anbieter einfach und kostengünstig bereitzustellen.

Aktuell eingesetzte Netzlösungen sind überwiegend Single-Lösungen, d.h. jedem Netz ist in der Regel ein eigener Dienst zugeordnet. Dabei ist die Netzintelligenz zum größten Teil hardwaremäßig mit jeweils eigener Technologie realisiert. Das bedeutet wenige Schnittstellen einerseits und „alles aus einer Hand" aus Sicht des Kunden andererseits. Sicherheit ist hierbei oft schon implizit erzielbar. In einem solchen Netz ist implizit klar, dass die Leitung nur vom autorisierten Nutzer verwendet werden kann, da nur dieser Zugang zu den Räumlichkeiten, in denen der Endpunkt installiert ist, haben sollte. Aus diesem Grund wird keine zusätzliche Identifizierung und Authentifizierung notwendig.

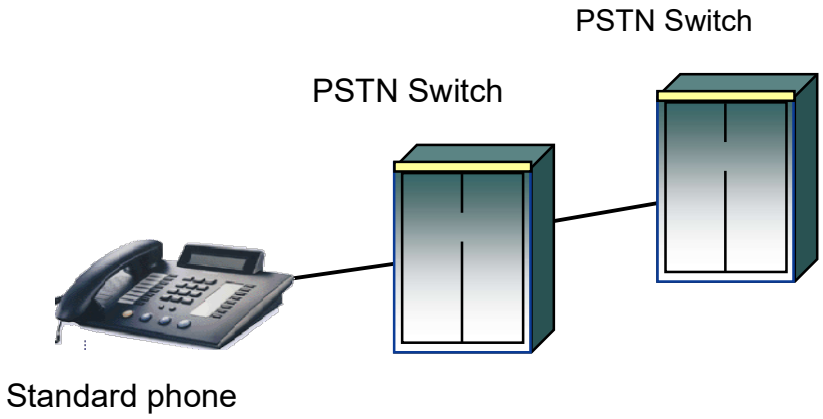

Abb. 2: Zuordnung eines Teilnehmers zu einem physischen Telefonanschluss (Trust by Wire)

Durch NGN wird das PSTN einen Wandel erfahren, der vergleichbar ist mit der Ablösung persönlicher Vermittlungsstellen durch automatisiertes Switching.

3 Zukünftige Netze (NGNs)

Abbildung 3 zeigt anschaulich, wie zentrale Dienste mit hoher Netzqualität in der Zukunft angeboten werden könnten und sollten.
Wichtig sind hierbei die grundsätzlichen Charakteristiken von Next Generation Networks (NGN).

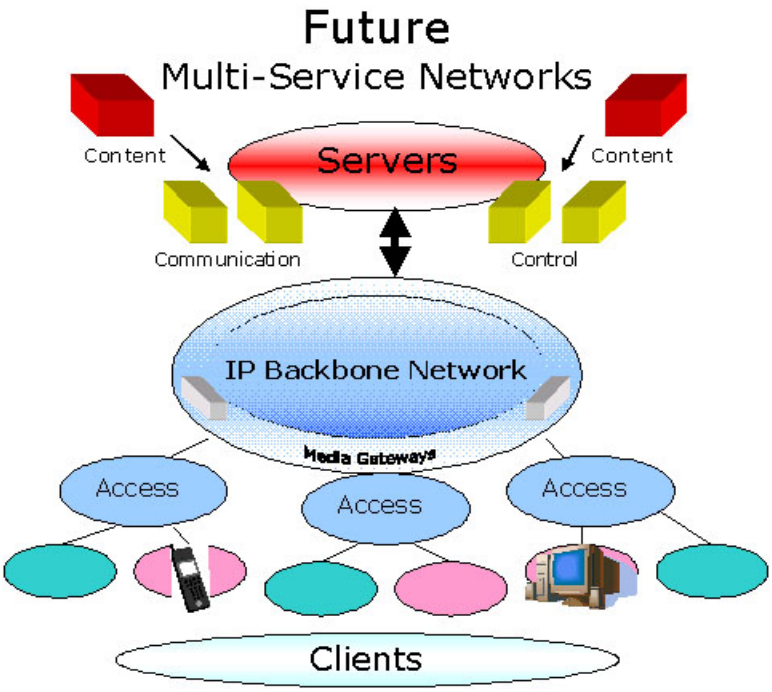

Abb. 3: Zukünftige Multimedia-Service-Netze

Ein NGN zeichnet sich vor allem durch ein Netzwerkkonzept aus, bei dem Multimedia, Echtzeitkommunikation und hohe Netzwerkintelligenz im Vordergrund stehen. Aus Sicht des Nutzers bietet ein NGN ein intelligentes Informationsmanagement und die Möglichkeit der individuellen Anpassung der Dienste an spezielle Anforderungen.

Ein solches Netz kann auch unterschiedlichste Übertragungsverfahren und Netzstrukturen in eine konvergente Netzwerkarchitektur überführen. Basierend auf der Paket-Technologie können jegliche Arten von Informationen und Daten transportiert werden. Die neuen Einsatzmöglichkeiten eines Multi-Service-Netzes erstrecken sich sowohl über Sprache, Daten und Video – und schaffen gleichzeitig zusätzliche Ressourcen für größere Bandbreiten oder Realzeitanwendungen. Dabei können bewährte asynchrone Kommunikationssysteme und elastische Anwendungen oder diskrete, zeitunabhängige Medien (z.B. Text und Grafik via E-Mail) ebenso eingesetzt werden wie kontinuierliche Echtzeitanwendungen (z.B. Audio/Video), bei denen sich die Werte zeitabhängig verändern und nur zu einem bestimmten Zeitpunkt gültig sind.

Die dadurch geschaffenen Möglichkeiten gehen jedoch gleichzeitig mit neuen, höheren Anforderungen in puncto Quality of Service einher.

Ein paketorientiertes Netz, das interaktive Echtzeit-Kommunikation abdeckt, muss auch für mehr Zuverlässigkeit und Ausfallsicherheit gerüstet sein, was nur durch Service-Differenzierung, sprich differenzierte Qualität (QoS) für verschiedene Dienste und Anwendungen, möglich sein wird.
Dabei sind permanente Erreichbarkeit in ausreichender Qualität und flächendeckende Online-Verfügbarkeit ebenso wichtig wie die Entwicklung und Integration von Management-Technologien, offenen Plattformen und Service-Schnittstellen.
Ein Next Generation Network ist somit eine Art „ALL IP-Netz", das alle damit verbundenen hohen Anforderungen erfüllen muss.

4 Sicherheitsanforderungen

Mit neuen technischen Möglichkeiten steigt in der Regel auch das Potenzial an Bedrohungen und damit das Risiko eines Schadens.
So werden zukünftig sehr viel mehr sensitive Informationen als Bits und Bytes generiert und verwaltet als es bisher der Fall war. Umso höher ist zukünftig die nachhaltige Einhaltung des Datenschutzes einzuschätzen, da ein mangelhafter Datenschutz dazu führen könnte und führen wird, dass die „unsicheren" Dienste vom Kunden nicht angenommen werden.

Je innovativer eine offene Architektur auf der einen Seite ist, desto größer wird die Gefahr durch unautorisierte Datenzugriffe von Dritten auf wertvolle und schützenswerte Informationen werden.
Um den Austausch sensibler Informationen zwischen unterschiedlichen Parteien sicher zu ermöglichen, wird es nötig sein, System und Medium entsprechend vor alten und neuen Angriffen zu schützen.
Ein wirksamer Medienschutz wird hierbei nur durch organisationsübergreifende Sicherheitsinfrastrukturen gewährleistet werden können.
Somit wird also die Berücksichtigung sämtlicher Aspekte des Datenschutzes und -sicherheit kritischer Erfolgsfaktor für neue Dienste und Applikationen werden!

Allgemein kann man sagen, dass sich durch die veränderten elektronischen Geschäftsprozesse auch neue Anforderungen und Notwendigkeiten bezüglich der Sicherheit und der Vertrauenswürdigkeit ergeben. Hier ist es unbedingt notwendig, eine passende Vertrauenswürdigkeit zu schaffen, damit das volle Potenzial ausgeschöpft werden kann.
Bestehende Dienste zeigen uns bereits heute schon gefährliche Grenzen auf, die an der Glaubwürdigkeit von modernen Technologien zu rütteln beginnen.
Die Bedrohungen, die wir zurzeit erleben und nicht wirklich beherrschen, resultieren aus Überraschungen und Ungewissheiten der komplexen und unübersichtlichen Informations- und Kommunikationssysteme.
Zwei – uns allen bekannte - Beispiele, die uns überrascht haben, und auf die wir uns nicht in Ruhe vorbereiten konnten, sind Spam-E-Mails und Passwort-Fishing.
Sicherheit ist notwendig, damit wir schon genutzte Dienste weiterhin verlässlich nutzen können, und damit das sehr große Potential, Geschäftsprozesse rationaler abzuwickeln, in der Zukunft noch genutzt werden kann.
Mit Vertrauenswürdigkeit und Sicherheit als Enabler, können wir weitere neue, innovative Dienste motivieren. Diese Sichtweise zeigt auf, dass allein die Vertrauenswürdigkeit und Sicherheit über Erfolg und Misserfolg neuer Dienste entscheiden kann.

Welchen Trend können wir bei der Sicherheit erkennen?
Wir erkennen eine Verschiebung der Konzentration von der klassischen „Perimeter Security", wie Firewall-Systeme, VPNs, Intrusion Detection Systeme, usw., die eine Reduzierung der Gefahren, die von außen kommen oder während

der Datenkommunikation über das Kommunikationsnetz auftreten können als Basis hatte, hin zur Anwendungssicherheit und zu Trusted Computing.

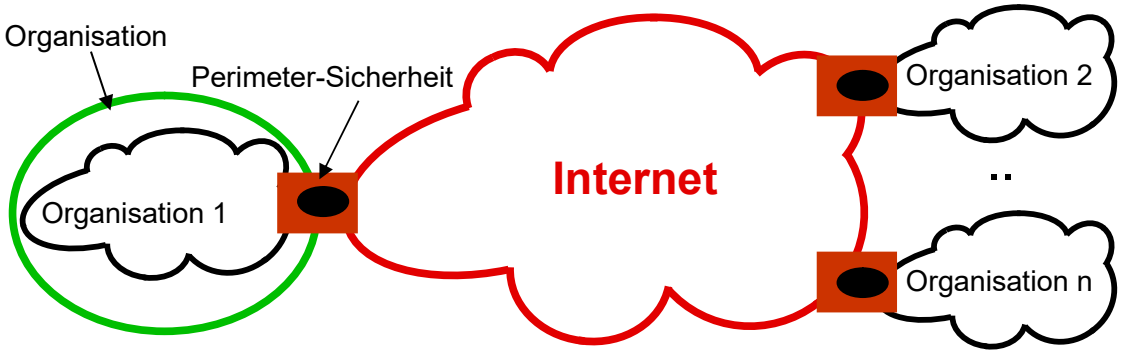

Abb. 4: Perimeter Sicherheit

Ziel der Anwendungssicherheit ist die Sicherheit von Objekten, die zwischen Anwendungen ausgetauscht werden und mit Hilfe von Objektverschlüsselung und digitaler Signatur vor Angriffen geschützt werden.

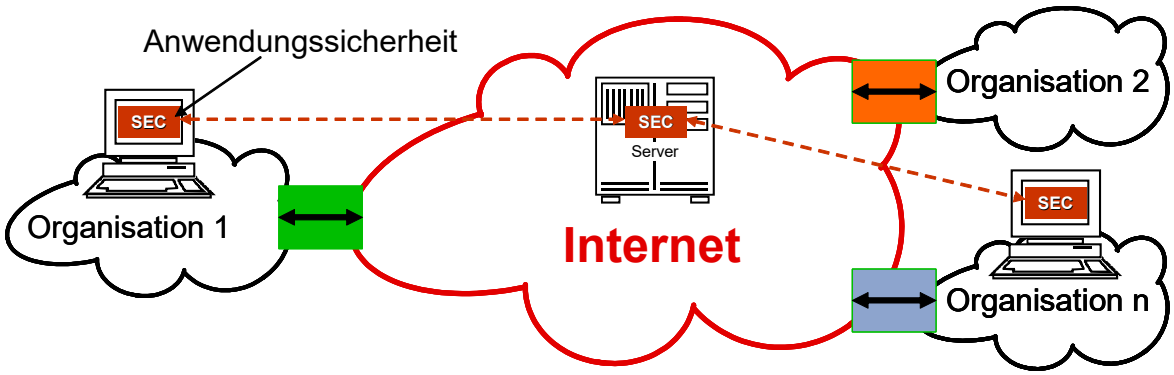

Abb. 5: Anwendungssicherheit

Trusted Computing versucht organisationsübergreifende sichere und vertrauenswürdige Sicherheitsplattformen zu etablieren, die in der Lage sind, eigene und fremde Sicherheitspolicies verlässlich umzusetzen.

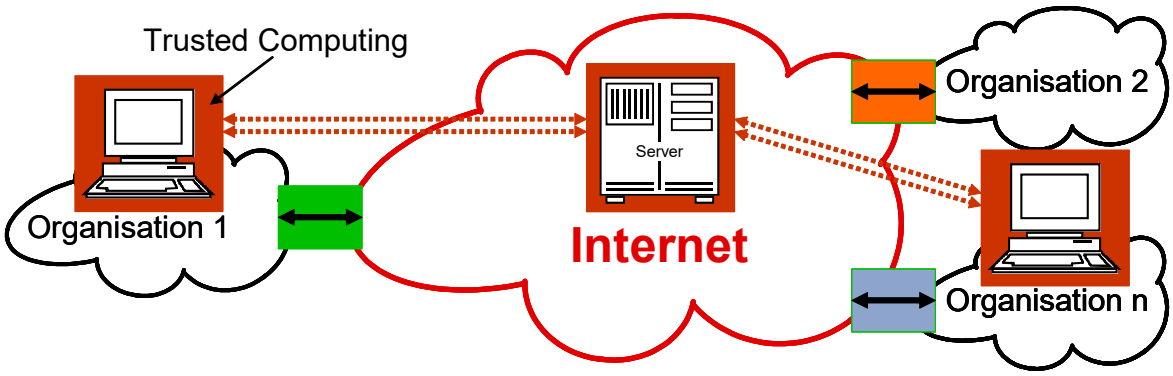

Abb. 6: Trusted Computing

Wichtig werden in Zukunft auch Kommunikationsanalyse- und Frühwarnsysteme werden, die uns helfen, schneller und effizienter in kritischen Situation, wie z.B. Viren- und Spam-Wellen und Denial of Service Attacken, zu reagieren.

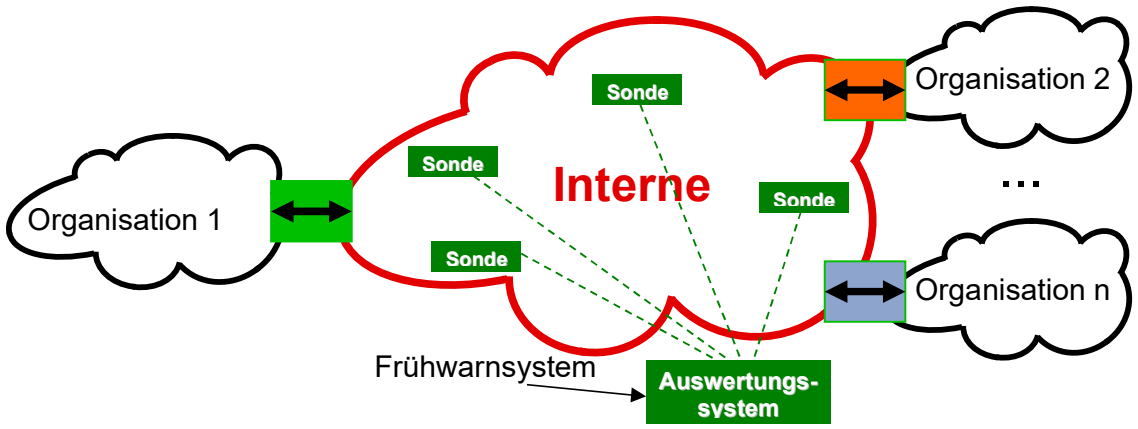

Abb. 7: Frühwarnsysteme

Nur neue zusätzliche Sicherheitskonzepte werden es ermöglichen, auch langfristig den Anforderungen an Sicherheit und Vertrauenswürdigkeit gerecht zu werden.

Welche Sicherheitsdienste sind insbesondere für NGN wichtig?
Zu allererst ist ein sicherer Zugang zum Network notwendig. Das umfasst sowohl Zugriffssicherheit über Breitband-Anschlüsse (z.B. DSL), als auch AAA (Authentication, Autorization, Accounting) für den mobilen Zugriff. Weitere wichtige Sicherheitsdienste sind, die Vertraulichkeit von Medien durch

entsprechende Verschlüsselung und die Verbindlichkeit von Geschäftsprozessen durch digitale Signaturen. Ein immer wichtigerer Sicherheitsdienst ist die Verfügbarkeit der Dienste im Sinne einer notwendigen Quality of Service für bestimmte Dienste. Dieser Quality of Service muss jedoch wiederum vor missbräuchlicher Nutzung geschützt sein muss. Bei QoS-Architekturen wie InteServ, DiffServ oder MPLS sind ernorme Umstrukturierungen in den Netzen notwendig. Neben den technischen QoS-Mechanismen wird ein Preismodell für die unterschiedlichen QoS-Level, das Abrechnen der erbrachten QoS-Leistungen und entsprechenden Kontrollmechansimen, die einen Missbrauch verhindern, umgesetzt werden müssen.
Eine daraus auch resultierende Forderung ist eine ganzheitlich sichere Managementinfrastruktur, die den hohen Anforderungen an ein sicheres NGN entsprechen.

Welchen Anforderungen müssen die Sicherheitsdienste genügen?
Wie brauchen skalierbare Sicherheiten, damit wir in der Lage sind maßgeschneiderte Sicherheitslösungen in Abhängigkeit von den Sicherheitsanforderungen der Benutzer anbieten zu können. Nicht jede Anwendung, nicht jeder Anwender hat den gleichen Schutzbedarf.
Wichtig ist auch die gleiche Benutzerschnittstelle für alle Zugriffe für eine praktikable Nutzung anzubieten. Ein weitere Anforderung ist es gleiche und standardisierte Sicherheitslösungen für alle Produkte, Anwendungen und Dienste zur Verfügung zu stellen, damit Sicherheit einheitlich und einfach umgesetzt werden kann. Die Sicherheitsdienste müssen sich den Bedürfnissen der Benutzer anpassen, sonst werden sie nicht genutzt.

5 Identity Management

Ein wichtiger Sicherheitsmechanismus für NGN ist aus der Sicht der Nutzer das Identity Management. Die Gefahren, die von dem Identitätsklau ausgehen, sind erheblich und stellen für die Zukunft ein sehr großes Risiko dar.
Jeder Anwender schleppt heutzutage einen Berg von Benutzernamen und Passwörtern mit sich herum. Sich alle zu merken ist schwierig, aber die Mehrfachverwendung ein und desselben Passworts ist zu unsicher. Die Anzahl der Dienste steigt stetig und mit ihr auch das Übel, sich bei jedem dieser Angebote erneut mit einem Benutzernamen und Passwort registrieren zu müssen.

Es gibt einige Möglichkeiten, wie diese Herausforderung durch Identity Management in Zukunft gelöst werden kann.

Für eine gesicherte Identität im Netz ohne das traditionelle Benutzername-und-Passwort-System kann z.B. eine zertifizierte One-Button-Klick-Through Technologie verwendet werden. Der User bedient dabei nur noch einen Button, um sich in einem gesicherten Bereich einer Webseite anzumelden. Client und Webserver tauschen z.B. per SLL ihre Zertifikate aus und prüfen diese. Das User-Zertifikat sollte dabei allerdings mobil in einem sicheren eToken und nicht auf einem Rechnersystem hinterlegt werden. Hierin wird sowohl das eigentliche Zertifikat gespeichert, sowie zusätzliche Funktionen, wie zum Beispiel das Single-Sign-On Prinzip per Zugangsdatenspeicherung.

Als vergleichende innovative Technik kann das Liberty Alliance Projekt genutzt werden. Hierbei schließen sich mehrere Service Provider zu einem „Circle of Trust" zusammen. Mit Hilfe dieser Technologie sind Single-Sign-On und Global Logout für viele Dienste auch unterschiedlicher Anbieter gleichzeitig möglich. Der Libertyansatz ist der Passport-Technologie von Microsoft sehr ähnlich, jedoch mit dem Unterschied der dezentralen Ausrichtung dieses Protokolls. Somit gibt es nicht einen „großmächtigen" Provider, der alle persönlichen Profile kennt, sondern lediglich eine Verlinkung der Profile */Linn05/*.

Mit Hilfe dieser Technologien können auch verschiedene Authentifizierungsarten nebeneinander gestellt und verglichen werden. In einem Forschungsprojekt hat das Institut für Internet-Sicherheit diese Technologien konkret auf unterschiedlichen Webseiten umgesetzt, um Erfahrungen zu sammeln. Hierbei sollen sowohl höhere Sicherheitsstufen erreicht werden, als auch die Usability für den Nutzer wesentlich verbessert werden (siehe Abb. 8).

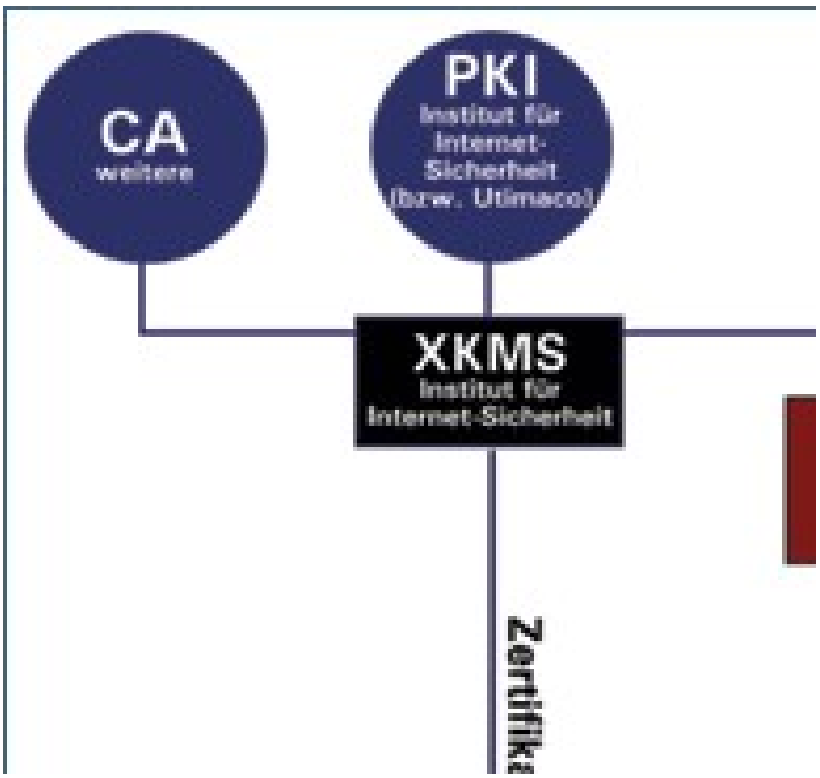

Abb. 8: Identity Management

Die Technologie, wie ein einheitliches Identity-Management realisiert werden kann, steht im Prinzip zur Verfügung. Die Aufgabenstellung, die wir so schnell wie möglich realisieren müssen ist, eine organisations- und länderübergreifende Sicherheitsinfrastruktur zu schaffen, damit die Technologie in der Masse umgesetzt werden kann. So können wir in diesem Bereich eine angemessene höhere Sicherheit und einen einfachen Zugang für Dienste schadensfrei nutzen. Die Ankündigung der Bundesregierung ab Ende 2006 einen digitalen Personalausweis mit Authentikationsfunktion zur Verfügung zu stellen, wird helfen, solche Technologien in der notwendigen Masse umzusetzen.

6 E-Mail-Verlässlichkeit

Der E-Mail Dienst ist einer der am weitesten verbreiteten und meist genutzten Dienste des Internets. Obwohl E-Mail zunächst nicht als verlässlicher Dienst konzipiert wurde, wird es heutzutage überwiegend als Mittel zur einfachen, nachrichtenbasierten und zuverlässigen Kommunikation im Internet eingesetzt. Der E-Mail Dienst ist für die Informationstechnologie inzwischen eine nicht mehr wegzudenkende Anwendung.

Seit einigen Jahren jedoch beeinträchtigen insbesondere Spam und Viren, aber auch andere Bedrohungen wie fehlende Vertraulichkeit das Medium E-Mail derart, dass fraglich ist, ob die heute so übliche E-Mail in der Zukunft noch genauso einfach, unkonventionell und produktiv eingesetzt werden kann.

Um letztlich das Gefahrenpotential für die E-Mail Nutzung konkret einschätzen zu können, hat das Institut für Internet-Sicherheit der FH Gelsenkirchen Ende 2004 eine Umfrage bei diversen Organisationen durchgeführt, die sowohl Aufschluss über die aktuelle Bedrohungslage durch Spam und Viren als auch über Maßnahmen zur Gefahrenabwehr geben sollte.

Dabei zeigten die erhobenen Zahlen einen deutlichen Handlungsbedarf:

Anhand der von den Organisationen zur Verfügung gestellten Zahlen des monatlichen Viren-Volumens konnte eine durchschnittliche Viren-Rate von 2,9% ermittelt werden. Vergleichswerte von spezialisierten Anbietern zeigten sogar einen deutlich höheren Viren-Anteil. Die ermittelte Spam-Rate spricht sogar eine noch deutlichere Sprache:

Der Anteil der unerwünschten Spam-Nachrichten am Gesamtaufkommen beträgt im Durchschnitt 61,5% aller E-Mails */DiPo05/*.

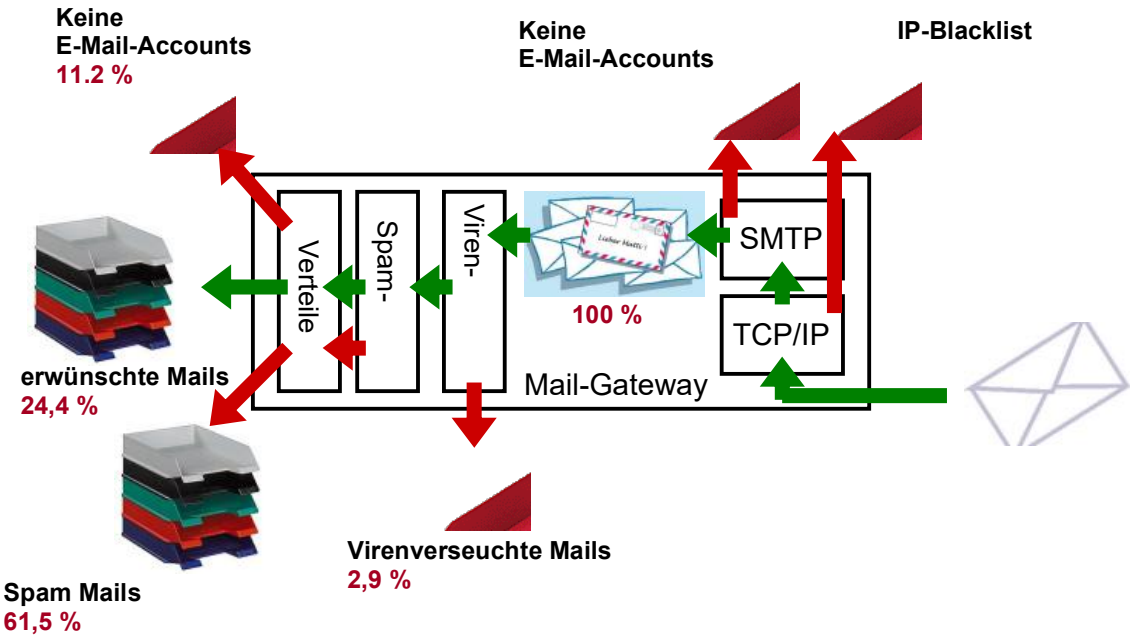

Abb. 9: Ergebnis der Umfrage E-Mail-Verlässlichkeit

Alle Befragten waren sich darüber einig, dass das Bedrohungspotential für Viren und Spam in der Zukunft steigen wird.

Interessant war dabei auch die Tatsache, dass anscheinend nur 4,3% aller E-Mails verschlüsselt und nur 6% signiert den Postausgang verlassen.

Da mehr als 43 % der Befragten angegeben haben, dass die E-Mail in kritischen Geschäftsprozessen verwendet wird, haben wir es mit einem sehr hohen Sicherheitsrisiko zu tun.

Außerdem hat die Umfrage ergeben, dass die derzeit eingesetzten Anti-Spam-Realisierungen die IP-Adressen nicht in den Griff bekommen, um den „Spammern" das Leben schwer zu machen.

Um diese Sicherheitsmankos in der Zukunft wirksam zu bekämpfen, werden mehr Ordnung und vor allem mehr Verantwortung seitens der Betreiber notwendig sein. Schwarze und weiße Listen, sowie Verschlüsselung und digitale Signaturen müssen zu Standards etabliert werden, um mittelfristig eine höhere Verlässlichkeit des Mediums E-Mail zu erreichen.

Die Sicherheitslösungen im Bereich E-Mail stehen zur Verfügung, sie müssen nur gemeinsam umgesetzt werden, um das Henne-Ei-Problem zu lösen.

7 Web Service Security

Eine weitere Sicherheitstechnologie stellt die so genannte Web Service Security dar. Ein Web Service ist ein Softwaresystem, das eine interoperable Maschine-zu-Maschine Interaktion über ein Netzwerk ermöglicht.
Ein Web Service-Softwaresystem kann Dienste dynamisch lokalisieren und binden. Dabei besteht eine lose Kopplung zwischen Provider und Consumer, sowie eine Interoperabilität.

Einsetzbare Sicherheitsmechanismen bei Web Services sind XML Signature und XML Encryption. Mit diesen Sicherheitsdiensten wird der Gefahr entgegengewirkt, dass Content gelesen und manipuliert werden kann.

Um die Verschlüsselung und Signatur von XML-Dokumenten sicher realisieren zu können, wird ein Verifikationsdienst für Zertifikate benötigt.

Dazu ist im W3C-Konsorzium der XKMS-Standard entstanden. XKMS besteht aus dem XML Key Registration Service (X-KRSS) und XML Key Information Service (X-KISS). XKMS beispielsweise bietet die Möglichkeit, den Funktionsumfang einer PKI als Web Service zur Verfügung zu stellen. Dadurch können auch Web Services die Funktionen einer PKI nutzen */BPP04/*.

Die X-KRSS Spezifikation definiert verschiedene Funktionen für die Verwaltung von Schlüsseln. Durch die Funktionen Register, Reissue, Revoke und Revover der X-KRSS Spezifikation kann der gesamte Lebenslauf eines Schlüssels mittels XKMS abgebildet werden.

An die X-KRSS Funktionen müssen dementsprechend besonders hohe Sicherheitsanforderungen gestellt werden, da die Funktionen zum Verwalten von Schlüsseln den Zertifizierungsrichtlinien entsprechen müssen. Das stellt heutige Web Services immer wieder vor Probleme und es zeigt sich, dass sich die Absicherung des Transportweges zur Sicherung von Web Services nicht immer als ausreichend erweist.
Nur der richtige Einsatz eines Web Service Systems und die sinnvolle Verknüpfung mit Sicherheitsfunktionen kann letztlich mit zu einer passenden und einfachen Sicherheitstechnologie beitragen.

8 Gemeinsame Sicherheitsinfrastruktur

Ob Identity Management, E-Mail-Sicherheit, Web Service Security, VPM-Systeme, usw., die meisten Sicherheitssysteme bauen auf so genannten Public-Key-Infrastrukturen (PKI) auf.

Während in den letzten Jahren viele PKIs in den Unternehmen eingerichtet wurden, die vordergründig die Anwenderseite im Fokus hatten, verschiebt sich die Entwicklung immer mehr in Richtung Interoperabilität der Systeme, damit ihr Nutzen voll ausgeschöpft werden kann. Bevor dieses Ziel erreicht werden kann, muss jedoch auf organisatorischer Seite (in Bezug auf verbindliche Leitlinien) noch die eine oder andere Hürde genommen werden.

Eine mögliche Lösung stellt das Konzept der Bridge-CA dar. Dabei wird eine Zertifizierungsstelle - die Bridge-CA - gebildet, die alle teilnehmenden CAs zertifizert. Die Bridge-CA ist jedoch keine Wurzelinstanz, sie zertifiziert lediglich die angeschlossenen Wurzelinstanzen. Damit die gegenseitige Anerkennung der teilnehmenden CAs gewährleistet ist, müssen alle CAs der Richtlinie der Bridge-CA entsprechen. Auf diese Weise wird eine "Brücke des Vertrauens" zwischen den PKIs gebildet, die eine sichere Kommunikation über Firmengrenzen hinweg ermöglicht. In Deutschland wurde unter Leitung des TeleTrust Vereins die European Bridge-CA ins Leben gerufen. Durch Bereitstellung verschiedener Dienste kann dort bereits heute die Kommunikation zwischen den angeschlossenen Teilnehmern sicher durchgeführt werden. Durch Teilnahme der Bundesverwaltung, der Deutschen Bank, der Deutschen Telekom, Siemens sowie vielen weiteren ist die European Bridge-CA auf einem guten Weg, zu einer wirklich vertrauenswürdigen CA-Plattform zu avancieren */Pohl04/*.

Zur Schaffung einer gemeinsamen Grundlage haben sich ebenfalls TeleTrusT e.V. und T7 e.V. mit Unterstützung durch das BMWi zusammen getan und die Spezifikation ISIS-MTT ins Leben gerufen.

Vorrangiges Ziel der Spezifikation ist dabei die flächendeckende Einführung PKI-gestützter Sicherheitstechnologien. Hierbei spielen Investitionssicherheit durch Kompatibilität zu internationalen Standards wie S/MIME, PKIX, PKCS, X.509, ETSI, CEN ESI usw. ebenso eine große Rolle, wie die enge Verzahnung mit der Bridge-CA-Initiative.

9 Gefahren der Zukunft?

Ein funktionierendes System bedeutet aber leider noch längst keine wirksame Sicherheit. Denn schneller als die Schutzmauern rund ums Netzwerk gebaut sind und die Werte auf dem Kommunikationsweg geschützt werden, haben sich bereits neue potentielle Gefahren eingeschlichen.
Somit ist es heute und auch zukünftig unumgänglich, die Sicherheitstechnologien ständig anzupassen und zu erweitern.
Ein sehr wahrscheinliches Problem, mit dem die Sicherheitssysteme über kurz oder lang umgehen müssen ist SPIT (Spam over Internet Telephony), sprich Reklameterror übers Internettelefon. Zwar wird es sich dabei aus Kostengründen vermutlich eher um gesprochene Audio-Werbebotschaften als um Live-Anrufe aus Call-Centern handeln, doch auch hier zeichnet sich schon jetzt die Stärke der Systeme ab: Laut US-Magazin „New Scientist" schafft es ein entsprechend programmierter Computer, bis zu 1000 Anschlüsse pro Minute anzurufen und seine gesprochene Reklame dem unfreiwilligen Zuhörer aufzubürden.

Die Angreifer der Zukunft kämpfen dabei mit alten und mit neuen Tricks und sind den Schutzmechanismen in der Regel immer einen Schritt voraus.
Auch Würmer und Viren werden in zukünftigen Sicherheitssystemen bedeutende Rollen spielen: Die Schädlinge werden dabei voraussichtlich nicht nur über E-Mails verteilt. Zunehmend nutzen sie auch die Schwächen in Netzwerkdiensten und falsche System-Konfigurationen aus. Um sich komplett über den Globus zu verteilen, brauchen E-Mail-Würmer schon heute nur noch etwa 24 Stunden. Netzwerkwürmer verbreiten sich selbstständig, unabhängig von Zeitzonen und Nutzerinteraktionen. Heute bekannte Bedrohungen für die Sicherheit wie Spam, Pishing oder Social Engineering werden auch in Zukunft eine große Rolle spielen – nur zeigt sich schon heute ein klarer Trend in Richtung Zunahme von Masse und Qualität der Gefahren.

10 Wie sicher ist „sicher"?

Bei so vielen Risiken und Gefahren, stellt sich unweigerlich die Frage, wie wirksam Sicherheitssysteme überhaupt sein können.

Ein grundsätzlich wichtiges Kriterium für die Beurteilung von Sicherheitssystemen ist die Frage danach, ob die Sicherheitssysteme auch tatsächlich in der Lage sind, den realen Angriffen entgegen zu wirken. Dabei kann die Stärke der eingesetzten Systeme unterschiedlich bewertet werden. Meist werden hier die Bewertungen hoch, mittel und niedrig verwendet. Eine wichtige Größe zur Bewertung von Sicherheitsmechanismen ist die Mindeststärke (SoMmin), die erforderlich ist, um allen Angriffen stand zu halten */Pohl03/*.

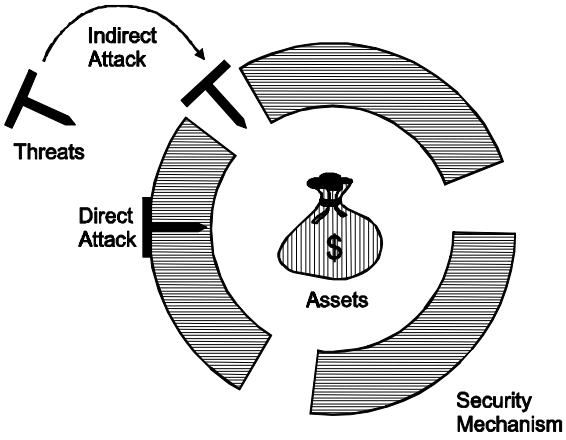

Abb. 10: Symbolische Darstellung der Wirksamkeit im Angriffsfall

Wichtige Kriterien für die Bewertung der Stärke sind dabei Fachkenntnisse, Ressourcen und Gelegenheit der potentiellen Angreifer.

Unter Fachkenntnisse fasst man alle Kriterien zusammen, die das Anwendungs-KnowHow des Angreifers beschreiben. Handelt es sich um einen Laien, einen versierten Benutzer (eine kenntnisreiche Person) oder gar einen Experten?

Ressourcen sind die für einen erfolgreichen Angriff erforderlichen Mittel. Dabei unterscheidet man die Komponenten Zeit und Ausstattung – die Zeit, die zur Durchführung des Angriffs benötigt wird und die erforderliche Ausstattung in Form von Hardware, Werkzeugen und Software.

So entstehen Bewertungsbandbreiten von „Sonderausstattung - innerhalb von Monaten" bis hin zu „Ohne Ausstattung – innerhalb von Minuten".

Das Bewertungskriterium „Gelegenheit" beschreibt im Gegensatz zu den anderen Punkten die eher schwer kontrollierbaren Gegebenheiten wie Zufall, geheime Absprachen und Entdeckung. Darunter fällt die eher zufällige Zusammenarbeit mit einem Anwender genauso, wie Absprachen mit dem eigentlich als vertrauenswürdig eingestuften Systemverwalter.

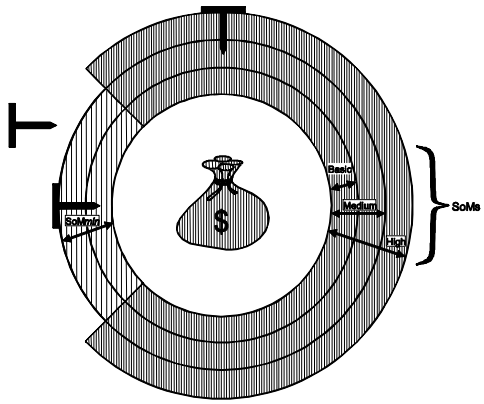

Abb. 11. Mindeststärke (SoMmin)

Daraus ergeben sich Sicherheitsbewertungen, die der jeweiligen Situation entsprechend greifen können.
So kann ein System, das innerhalb von Minuten von einem Laien alleine überwunden werden kann, wohl nicht einmal mehr als „niedrig" eingestuft werden. Jedoch könnte man ein System, das nur mittels Sonderausstattung und in monatelanger Expertenarbeit in die Knie gezwungen werden kann, als „hoch" einstufen.
Ein weiteres Kriterium zur Beurteilung eines Sicherheitssystems ist die Korrektheit.
Mit dem Faktor Korrektheit soll überprüft und beurteilt werden, ob die Sicherheitsmechanismen korrekt implementiert sind und wie groß das Vertrauen in die Implementierung der Lösungen ist.
Grundsätzlich kann also gesagt werden, dass IT-Systeme nur als wirklich sicher eingestuft werden können, wenn Wirksamkeit, Stärke und Korrektheit zu gleichen Teilen in angemessener Qualität vorherrschen.

11 Eine Frage der Vertrauenswürdigkeit

IT-Sicherheitssysteme werden zu einem großen Teil an ihrer Wirksamkeit, Stärke und Korrektheit gemessen - bleibt also am Ende doch alles eine Frage der Vertrauenswürdigkeit?

Ja, denn Vertrauenswürdigkeit schafft Sicherheit – Sicherheit in dem Sinne, dass wir IT-Produkte länger und vor allem risikoärmer nutzen können. Sie sorgt für das nötige Zutrauen in die Hersteller, die Netz- und Serviceprovidern eine

verlässliche und sichere IT-Technologie zur Verfügung stellen, was in der jungen Vergangenheit in der IT-Branche leider nicht immer der Fall war.
Vertrauen ist eben mehr als nur der gute Glaube in Technologie und Gesetze – Vertrauen kann und muss wachsen und dabei werden jetzt und zukünftig Zuverlässigkeit, Gewissheit und Glaubwürdigkeit zentrale Rollen spielen.
Mit Zuverlässigkeit ist gemeint, dass die IT-Produkte und Lösungen nur die Dinge tun, die gewünscht sind - und das möglichst zu 100% zuverlässig.
Gewissheit beschreibt dabei das „gute Gefühl", dass sich jemand um die Sicherheitsfragen und auch alle anderen Aspekte der Vertrauenswürdigkeit kümmert, während die Glaubwürdigkeit in die Aussagen, die gemacht werden, und in die Aktivitäten, die im Bereich der IT getan werden, um mehr Sicherheit und mehr Vertrauenswürdigkeit zu erlangen, zu jeder Zeit gegeben sind.
Diese und zusätzliche Aspekte wie Aufrichtigkeit, Pflichtbewusstsein, Gewissenhaftigkeit und Verantwortlichkeit schaffen überhaupt erst eine passende Vertrauenswürdigkeit und sind letztlich der Schlüssel zu einem funktionierenden Sicherheitssystem.
Wir dürfen die neuen Möglichkeiten, die uns geboten werden, nicht leichtsinnig verspielen, weil wir nicht vertrauenswürdig sind.

12 Wer hat die Macht?

Ein weiterer Aspekt, der mit der zunehmenden Nutzung des Internets, betrachtet werden muss, ist die Frage der Macht.
Die Macht kann aus mehren Blickwinkeln betrachtet werden: Marktmacht, Nutzermacht und politische Macht. Die Markmacht kann z.B. die Macht über Inhalte sein. Hier hat Google mit einem Marktanteil von 47,3 % (Yahoo 20,9 %, MSN 13,6 %, AOL 4,5 %, usw.) eine exponierte Stellung. Es gibt aber auch die Marktmacht über Anwendungen, wie z.B. des Monopolisten Microsoft im Bereich der Browser. Hier hat Microsoft mit dem Internet Explorer einen Marktanteil von ca. 70 % (Firefox 25%, Opera 1,8%, Netscape 1%, usw.).
Die Macht des Nutzers wird durch das „End-to-End-Prinzip" des Internets bestimmt. Das Internet kennt keine zentrale Steuerung von Datenflüssen, kennt keine Diskriminierung von Anwendungen. Aus dieser Betrachtung heraus ist das Internet ein „dummes Netz". Die Folge ist, die Macht der Internetnutzer ist größer als die der Telefonkunden. Damit haben wir es mit einer großen

Innovationsdynamik zu tun. Aber es gibt eben erwünschte und unerwünschte Innovationen, wie z.B. Viren, Trojaner, usw.
Die politische Macht ist ein eher schwieriges Thema. Das Internet geht über alle geographischen Grenzen, politischen/administrativen Grenzen und Kulturen hinaus und stellt somit eine neue und ungewohnte Herausforderung für die internationale Gesellschaft dar. Bis Mitte der 90er Jahre regierten die Ingenieure das Internet. Die Privatisierung der Netzinfrastrukturen führte z.B. zu Konflikten um Domainnamen: Ist das DNS ein öffentliches Gut? Gilt im Internet das Markenrecht? Wer bestimmt über die Zukunft des DNS? Wo und durch wen sollen diese Fragen verhandelt werden?
Die ICANN als Experiment in globaler Willensbildung ist der erfolglose Versuch „Macht von unten" in Form von Selbst-Regulationen zu institutionalisieren.
Die Zukunft der unterschiedlichen Machtverhältnisse ist von entscheidender Bedeutung für die Stabilität und die Weiterentwicklung des Internets.

13 Fazit

Die Praxis zeigt uns, dass wir gerade im Bereich der Netzwerk-/Internet-Sicherheit noch vor große Herausforderungen gestellt sind. Die neuen Dienste, die uns angeboten werden bescheren uns einerseits einen wesentlich höheren Aktionsradius, andererseits aber auch eine starke Abstraktion zwischen Handlung und Wirkung. Das erfordert einen deutlich behutsameren und bewussteren Umgang mit den Möglichkeiten, die uns die neue virtuelle Welt bietet.
Eine Veränderung unserer Kultur und eine Anpassung des Rechtssystems werden in kurzer Zeit schon unumgänglich werden, wenn wir uns zukünftig in dieser veränderten, modernen Welt zu Recht finden wollen.
Dazu wird insbesondere eine umfassende Aufklärung über die Risiken und Gefahren notwendig sein, sowie Schulungen für einen bewussten, richtigen Umgang mit den neuen Medien. Man könnte sogar die Möglichkeit diskutieren, ob es nicht sinnvoll wäre, einen „Internet-Führerschein" einzuführen, der uns optimal auf die Möglichkeiten und Gefahren vorbereitet.
Dabei sollen keine unnötigen Ängste produziert werden, sondern klar und deutlich über die Möglichkeiten, aber auch die Risikofaktoren aufgeklärt werden.
Ein weiterer Schritt in eine optimierte Zukunft ist die Einführung einer neuen Ordnung mit den dazugehörigen Regeln. Wir alle brauchen Regeln, um zum

Beispiel von einem Ort zum anderen zu kommen. Im Straßenverkehr befolgen wir bereits viele Regeln – warum nicht auch im Internet?

Das rasante Wachstum des Internets ist zwar zu einem großen Teil den Freiräumen zu verdanken, doch sind wir heute an einem Punkt angelangt, an dem sich die Rahmenbedingungen für das Wirken und Schaffen im Internet geändert haben. Das Internet ist längst kein Exot mehr, dessen Entwicklung hin und wieder mit Interesse beobachtet wird, sondern vielmehr leben wir als Gesellschaft bereits in einer gewissen Abhängigkeit zu dem „neuen" Medium.

Wir müssen es in Zukunft durch reglementierendes Eingreifen schaffen, die positiven Kräfte vor den negativen Kräften, wie z.B. Spammern zu schützen.

Wir benötigen langfristige Sicherheitsmechanismen, die unsere Systeme schützen, aber nicht einschränken. Dazu brauchen wir zukünftig zusätzlich einerseits Frühwarnsysteme, die die Reaktionszeiten in kritischen Situationen verringern und andererseits sichere Betriebssystemplattformen für neue vertrauenswürdige Anwendungen, damit neue Innovationen mit der dazu notwendigen Sicherheit auch zukünftig realisiert werden können.

Sicherheit darf nicht zum Luxus werden, sondern muss flächendeckend realisiert werden – damit wir uns auch in Zukunft noch mit gutem Gewissen in den Netzen dieser Welt frei bewegen können.

14 Literatur

/DiPo05/ C. Dietrich, N. Pohlmann: „eMail-Verlässlichkeit – Verbreitung und Evaluation", in "DACH Security 2005", Hrsg.: Patrick Horster, syssec Verlag, 2005

/BPP04/ D. Bär, A. Philipp, N. Pohlmann: „Web Service Security - XKMS", in "Securing Electronic Business Processes - Highlights of the Information Security Solutions Europe 2004 Conference", Hrsg.: S. Paulus, N. Pohlmann, H. Reimer, Vieweg-Verlag, Wiesbaden 2004

/Pohl03/ N. Pohlmann: "Firewall-Systeme - Sicherheit für Internet und Intranet, E-Mail-Security, Virtual Private Network, Intrution Detection-System, Personal Firewalls", MITP-Verlag, Bonn 2003

/Pohl04/ H. Blumberg N. Pohlmann: "Der IT-Sicherheitsleitfaden", MITP-Verlag, Bonn 2004

/Linn05/ M. Linnemann: "Identity Management", Diplomarbeit, Institut für Internet-Sicherheit, FH-Gelsenkirchen 2005

15 Verfasserportrait

Norbert Pohlmann studierte von 1981 bis 1985 Elektrotechnik mit dem Schwerpunkt Informatik in Aachen. Von 1997 bis 2001 Dissertation zum Thema „Möglichkeiten und Grenzen von Firewall-Systemen". Er war von 1985 bis 1988 Forschungsingenieur und später Leiter des Labors für Telematik an der Fachhochschule Aachen. Ab 1988 war er geschäftsführender Gesellschafter der Firma KryptoKom, Gesellschaft für kryptographische Informationssicherheit und Kommunikationstechnologie mbH. Nach der Fusion der KryptoKom mit der Utimaco Safeware war er von 1999 bis 2003 Mitglied des Vorstandes der Utimaco Safeware AG. Seit dem Wintersemester 2003 ist er Professor im Fachbereich Informatik, Studienrichtung „Internet und mobile Netze" mit dem Lehr- und Forschungsgebiet „Verteilte Systeme und Informationssicherheit" und seit 2005 ist er geschäftsführender Direktor des Instituts für Internet-Sicherheit (ifis) an der Fachhochschule Gelsenkirchen, das sich hauptsächlich den Gebieten Internet-Erforschung, E-Mail Sicherheit, Internet-Recht, Web-Service Sicherheit und Trusted Computing widmet.

Norbert Pohlmann befasst sich bereits seit 1985 mit IT-Sicherheit und Kryptographie sowie ihren Anwendungsgebieten. Als Gründungsmitglied 1989 und seit April 1997 als Vorstandsvorsitzender von TeleTrusT e.V., hat er sich die Etablierung von vertrauenswürdigen IT-Systemen zur Aufgabe gemacht.

Norbert Pohlmann ist Träger des Preises der Stadt Aachen für Innovation und Technologie von 1997 und ist Mitinitiator der "Information Security Solutions Europe"-Konferenz (ISSE) und Vorsitzender des Programmkomitees.

Institut für Internet-Sicherheit
FH-Geslenkirchen
Neidenburgerstraße 43
45877 Gelsenkirchen
www.internet-sicherheit.de