Das Projekt Janus wurde aus Mitteln des IT-Sicherheitsforschungsprogramms (Zukunftsfonds) finanziert, mit dem das BSI prioritäre Fragestellungen aus der sich ändernden Bedrohungslage präventiv adressiert.

Die Einführungsphase von Janus bei den ersten Bundesbehörden ist positiv und konstruktiv verlaufen. Um die individuellen Anforderungen der Behörden noch besser unterstützen zu können, befinden sich weitere Leistungsmerkmale in der Planung. Auch eine Kombination der Janus-Schleuse mit einer optimierten Hardware (Appliance mit Touchscreen) wird vorbereitet. Damit kann der Aufwand hinsichtlich Administration und Wartung minimiert und die Benutzerakzeptanz noch weiter verbessert werden.

Janus kann für die Bundesverwaltung kostenfrei über janus@bsi.bund.de bezogen werden – unter dieser Adresse sind auch weitere Informationen zum Projekt abrufbar. ■

Sicherheitsaspekte bei der elektronischen Übertragung von Nachrichten

Die öffentliche Meinung basiert zu einem wesentlichen Teil auf Nachrichten, die von nationalen und internationalen Presseagenturen recherchiert, gesammelt und auf elektronischem Weg an die Medien weitergeleitet werden. Einzelne Nachrichten können dabei kurzfristig gravierende Reaktionen bewirken, zum Beispiel Börsenstürze, Panik in der Bevölkerung oder politische Fehlentscheidungen. Bei der elektronischen Übermittlung muss daher durch technische Maßnahmen sichergestellt werden, dass die Nachrichten nicht von Dritten manipuliert werden können beziehungsweise dass ihre Authentizität durch den Empfänger in eindeutiger Weise überprüfbar ist.

Von Herbert Blum, BSI

Glauben Sie alles, was in der Zeitung steht? – „Natürlich nicht!" würden wohl viele spontan auf diese Frage antworten, denn wie die Erfahrung zeigt, ist ein gesundes Maß an Skepsis gegenüber dem, was oft als „veröffentlichte Meinung" bezeichnet wird, durchaus angebracht. Mit der Entscheidung allerdings, welche Nachricht als glaubwürdig einzustufen ist und welche nicht, wird sich im konkreten Fall oft auch der „mündige Bürger" nicht leicht tun. Außer Plausibilitätsbetrachtungen auf Basis des „gesunden Menschenverstandes" stehen ihm kaum objektive Kriterien zur Verfügung, um den Wahrheitsgehalt von Medienberichten verlässlich zu beurteilen. Allenfalls durch den Vergleich der Berichterstattung zu einem Ereignis in voneinander unabhängigen Medien lässt sich deren Zuverlässigkeit bis zu einem gewissen Grade objektiv überprüfen. Doch gilt auch dies nicht ohne Vorbehalte, denn meist stammen die Nachrichten, welche Funk-, TV- oder Print-Medien scheinbar vollkommen unabhängig voneinander verbreiten, doch aus der gleichen Quelle, nämlich einer der großen nationalen oder internationalen Nachrichtenagenturen.

Ähnlich zu anderen Konsumgütern, wie Lebensmitteln, Kleidung, Elektroartikeln und so weiter, wird der Endverbraucher mit der Ware „Nachricht" über ein Vertriebssystem aus Groß- und Einzelhändlern beliefert. Zwar sind die „Einzelhändler" – Zeitungen, TV- und Rundfunkanstalten – teilweise auch Produzenten der von ihnen vertriebenen Ware, indem sie Nachrichten und Hintergrundberichte über die eigenen Redaktionen selbst recherchieren. Den weitaus überwiegenden Teil der Meldungen – größenordnungsmäßig einige tausend pro Tag – beziehen diese Medien jedoch von den Großhändlern dieses Marktes, den Nachrichtenagenturen.

Übertragung und Manipulation

Die Übermittlung der Nachrichten erfolgt in der Regel auf elektronischem Weg. Ohne hinreichende Sicherheitsmaßnahmen besteht dabei die Gefahr, dass die Daten von „interessierter Seite" manipuliert beziehungsweise so genannte Hoaxes, also Falschmeldungen, in die Welt gesetzt werden.

Die Authentizitätsprüfung über eine elektronische Signatur hätte so beispielsweise folgenden Hoax verhindert: Am Neujahrstag 2006 erhielt die Nachrichtenagentur Associated Press (AP) per E-Mail die Pressemitteilung eines „Bundes Deutscher Juristen" (BDJ), in der dessen Vorsitzender, angeblich Strafrichter am Bundesgerichtshof, sich dafür aussprach, im Zuge der Terrorbekämpfung zur Erzwingung von Aussagen auch das Mittel der „leichten Folter" einzusetzen. Da dieses Statement gut zu einer zu jener Zeit stattfindenden politischen Diskussion passte, gelangte die Nachricht in die Medien und sorgte kurzfristig für einige Verwirrung. Es scheint fast überflüssig zu bemerken, dass weder der angebliche Bundesrichter noch der BDJ je existierten, obwohl für letzteren bis heute eine Internet-Seite bei einem Provider in den USA gehostet wird.

Neben politischen Motiven stehen hinter manipulierten Nachrichten oft auch handfeste materielle Interessen. So schaffte es im Jahr 2000 ein 23-jähriger Student und Aktienspekulant, den Kurs des an der amerikanischen Technologiebörse NASDAC notierten Unternehmens Emulex auf Talfahrt zu schicken: Innerhalb von 15 Minuten stürzte das Papier um 60 % von 110 US-$ auf 43 US-$ ab. Ursache hierfür war wieder eine per E-Mail verbreitete gefälschte Pressemitteilung, in der das Unternehmen eine Gewinnwarnung herausgab. Der Gewinn des auf fallende Kurse spekulierenden Urhebers der Falschmeldung belief sich auf rund 250.000 US-$. Demgegenüber schlugen bei anderen Anlegern, die ihre Aktien im Verlauf des Kurssturzes panikartig verkauften, Verluste von insgesamt zirka 100 Mio. US-$ zu Buche. Daraus resultierten dann 2001 auch Schadensersatzklagen dieser Anleger gegen die Agentur Bloomberg, welche die gefälschte Meldung mit verbreitet hatte.

Anforderungen

Das Nachrichtengeschäft basiert vor allem auf dem Faktor Zeit: Meldungen sollen so schnell wie möglich weiterverbreitet werden und keine Zeitung, keine TV- oder Radiostation möchte später beliefert werden als ihre Konkurrenten. Weiterhin müssen die Übertragungswege robust gegen Störungen und möglichst redundant ausgelegt sein. Schließlich und vor allem muss der Empfänger stets sicher sein können, dass die erhaltenen Informationen authentisch sind. In Stichpunkten zusammengefasst ergeben sich also die vier folgenden Anforderungen an die Nachrichtenübermittlung:

- Schnelligkeit,
- Gleichzeitigkeit,
- Ausfallsicherheit,
- Authentizität.

Da Nachrichten sowieso zur Veröffentlichung bestimmt sind, spielt die Vertraulichkeit der Übertragung im Normalfall eine eher untergeordnete Rolle und soll hier daher nicht im Fokus der Betrachtung stehen.

Die drei ersten Anforderungen – Schnelligkeit, Gleichzeitigkeit und Ausfallsicherheit – lassen sich nur mithilfe einer globalen, möglichst redundant ausgelegten Netzinfrastruktur realisieren. Terrestrisch bietet sich hier natürlich das Internet an, extraterrestrisch die Satellitenübertragung. Ursprünglich für die militärische Kommunikation entwickelt, wurden beide Netze speziell im Hinblick auf die drei genannten Anforderungen konzipiert. Ältere Verfahren wie Telefax oder ISDN kommen heute zwar auch noch zum Einsatz, sollen hier jedoch nicht mehr betrachtet werden.

Satellitenübertragung

Bereits vor dem Anfang des in den 1990er-Jahre einsetzenden Booms des Internets hatte sich die Satellitenkommunikation als Broadcast-Dienst für die Übertragung von (Presse-)Nachrichten etabliert. Die von den Agenturen gelieferten Meldungen werden dabei von einer Bodenstation an einen Satelliten gefunkt, der die Signale in einen großflächigen Bereich zur Erde zurück reflektiert. Dort werden sie von den Receiver-Anlagen der Medien sowie auch staatlicher Einrichtungen (z. B. Pressestellen von Ministerien, Katastrophenschutz) empfangen (s. Abb. 1) und in die Redaktions-systeme eingespeist. Wie beim privat genutzten Satelliten-TV, erfolgt die Übertragung durch Geräte vom Typ „GEO" (Geostationary Earth Orbit), die sich in zirka 36 000 km Höhe synchron zur Erdrotation auf einer Kreisbahn um den Äquator bewegen. Von der Erde aus gesehen erscheinen diese Satelliten ortsfest, weshalb die Antennen nur einmal ausgerichtet werden müssen und danach keiner weiteren Korrekturen mehr bedürfen.

Bedingt durch die Entfernung des Satelliten, sind die von den Signalen zurückzulegenden Wege gegenüber der terrestrischen Übertragung um ein Vielfaches länger, was zu einem Laufzeitverlust von etwa einer Viertelsekunde führt. Während sich diese Signalverzögerung bei interaktiven Sprachdiensten als störend erweist (viele Mobilfunk-Satelliten werden daher auf erdnahen Bahnen betrieben, sog. LEOs = „Low Earth Orbits"), fällt sie bei der Nachrichtenübermittlung kaum ins Gewicht. Begrenz-

ender Faktor für die Übertragungsgeschwindigkeit ist hier vielmehr die zur Verfügung stehende Bandbreite.

Satellitenkommunikation nutzt zur Datenübertragung das so genannte Ku-Band, welches dem Frequenzbereich zwischen 12–18 GHz entspricht. Die Bandbreite eines Satelliten-Transponders, des Gerätes also, das die Daten des Senders auffängt und an die Empfänger weiterleitet, beträgt im Ku-Band typischerweise 36 MHz. Diese Bandbreite entspricht unter realistischen Umständen einer Übertragungsrate von etwa 40 Mb/s.

Pressemeldungen werden gewöhnlich als Text- oder Bilddateien, in geringerem Umfang auch im Audio-Format (MPEG2) übertragen. Von den bis zu 10 000 Textnachrichten und etwa 2000 Bildern, die eine große Nachrichtenagentur täglich liefert, bilden letztere mit etwa 2 GB den weitaus größten Anteil am Datenaufkommen. Um dieses zeitnah zu übertragen, ist eine Übertragungsrate in der Größenordnung von 1 Mb/s, also etwa 1/40 der Kapazität eines Transponders, ausreichend, zumal durch Datenkompression und Multiplex-Verfahren, bei denen man die Übertragungskapazität lastabhängig unter den gesendeten Nachrichtenpaketen aufteilt, die zur Verfügung stehende Bandbreite weiter optimiert wird. Die Anforderung der gleichzeitigen Versorgung jedes Kunden ist dabei aufgrund des weiträumigen Ausleuchtkegels der Satelliten in nahezu perfekter Weise erfüllt (s. Abb. 1).

Auch die Ausfallsicherheit ist in hohem Maße gewährleistet, da Satelliten auf ihren Umlaufbahnen autarke Systeme bilden. Störungen in terrestrischen Infrastrukturen (z. B. Stromausfälle oder starke Gewitter) können höchstens lokale Sende- und Empfangseinrichtungen in ihrer Funktionstüchtigkeit beeinträchtigen, das Übertragungsnetz selbst bleibt davon jedoch unberührt. Großflächig oder auf längere Zeit vermögen „irdische Katastrophen" der Satellitenkommunikation kaum etwas anzuhaben. Gefahren für das System können allerdings „kosmischen" Ursprungs sein, zum Beispiel Einschläge von Meteoriten oder „Weltraumschrott" in einzelne Satelliten oder durch besonders starke Sonnenaktivität (sog. Flares) ausgelöste elektromagnetische Stürme. Da solche Ereignisse im Vergleich zu Erdbeben, Stürmen, Flutkatastrophen und so weiter weitaus seltener vorkommen, hat sich das Satellitennetz gegenüber den irdischen Kommunikationssystemen als sehr robust erwiesen. Einzelne Staaten, wie Japan, haben aus diesem Grund sogar per Gesetz festgelegt, dass im Katastrophenfall die Kommunikation über Satelliten erfolgen muss.

Im Gegensatz zu terrestrischen Netzen liegt bei der Satellitenkommunikation die Übertragungsstrecke größtenteils außerhalb der Zugriffsmöglichkeiten eines potenziellen Angreifers, der die Absicht hat, Daten zu manipulieren: Spoofing-Attacken mit dem Ziel, gefälschte Nachrichten in das System zu lancieren, können daher höchstens im direkten Umfeld des Senders oder des Empfängers erfolgen.

Geht man davon aus, dass die Übertragungsnetze zwischen Agentur und Sendeanlage sowie zwischen Receiver und Redaktionssystem nach außen abgeschottet sind (was natürlich sichergestellt sein muss), so bleibt dem Angreifer nur die Möglichkeit, die gefälschten Daten entweder über einen eigenen Sender zur Weiterverbreitung an den Satelliten zu schicken oder sie direkt in die Antenne des Empfängers einzustrahlen. Allein der apparative Aufwand, um das individuelle Signal eines Senders in Codierung, Multiplexing, Modulation und so weiter exakt so nachzubilden, dass die entsprechend konfigurierte Empfangsanlage die gefälschten Datenframes als fehlerfrei akzeptiert, ist so hoch, dass der Angreifer sich die entsprechenden Gerätschaften höchstens durch Diebstahl beschaffen könnte. Selbst wenn dies gelänge, müsste der Angreifer im ersten Fall weiterhin über eine Sendeanlage verfügen, deren Leistung so hoch ist, dass sie das Signal der regulären Bodenstation vollständig überdeckt – allein die dafür benötigte Parabolantenne hätte einen Durchmesser von mehr als 5 m.

Das Einstrahlen manipulierter Daten direkt in die Antenne

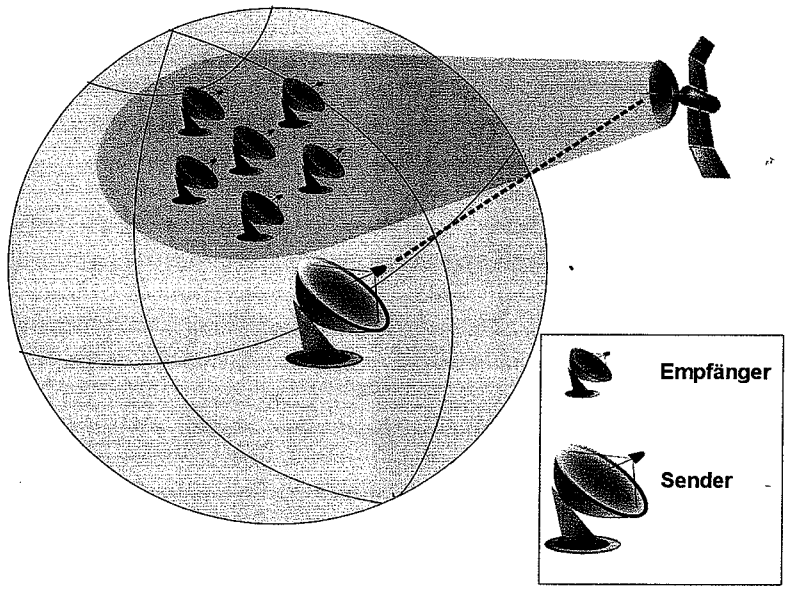

Abbildung 1: Bei der Satellitenkommunikation wird das Signal des Senders vom Satelliten großflächig zur Erde zurück reflektiert.

des Empfängers ließe sich gegebenenfalls aus einem Heißluft- oder Gasballon heraus bewerkstelligen. So skurril ein solches Szenario bereits im Ansatz erscheint, so gering ist in der Praxis die Aussicht auf einen Erfolg des Angriffs: Das Fluggerät wäre über einen hinreichenden Zeitraum auf die exakte Position des Satelliten zu fixieren, die eingestrahlte Leistung müsste genau der des Satelliten entsprechen und es dürfte zu keinen Interferenzen mit dessen Signalen kommen, da dies den Angriff sofort offensichtlich werden ließe.

Was also die Verfügbarkeits- und sicherheitstechnischen Anforderungen betrifft, erscheint die Satellitenkommunikation zunächst als das nahezu ideale Übetragungsmedium. Allerdings steht dem ein entscheidender Nachteil gegenüber: der materielle Aufwand sowie die relativ hohen Kosten, welche für die permanente Bereitstellung von Satellitenkanälen einer hinreichenden Bandbreite anfallen. Hier bieten terrestrische Netze, insbesondere das Internet, natürlich große Vorteile.

Übertragung via Internet

Ursprünglich konzipiert wurde das Internet zu militärischen Zwecken als ein hoch rendundant ausgelegtes Kommunikationsnetz, welches einen Datenaustausch auch dann noch gewährleisten sollte, wenn infolge kriegsbedingter Einwirkungen Teile dieses Netzes zerstört würden. Bedingt durch die rasante Entwicklung der letzten beiden Jahrzehnte wurden die Maschen dieses Netzes immer enger geknüpft, wodurch die Redundanz der Übertragungswege und damit die Verfügbarkeit des gesamten Netzes stetig zunahmen. Unter den terrestrischen Netzen verfügt das Internet somit wohl über die höchste Ausfallsicherheit.

Die für die Nachrichtenübermittlung per Satellit benötigte Bandbreite von etwa 1 Mb/s erscheint im Vergleich zu den Kapazitäten, die das Internet bietet, auf den ersten Blick recht bescheiden. Zu beachten ist hierbei jedoch, dass es sich bei der im letzten Abschnitt beschriebenen Form der Satellitenkommunikation um einen echten Broadcast-Dienst handelt, das heißt trotz der geringen Bandbreite erreichen die Daten zur gleichen Zeit eine im Prinzip beliebig große Zahl von Empfängern. Holen sich hingegen die Kunden ihre Daten alle zur gleichen Zeit bei einem Internet-Server ab, so benötigt dieser gegenüber dem Satelliten die *n*-fache Bandbreite, wobei *n* die Zahl der Empfänger bezeichnet. Um also die Forderung nach einer schnellen und gleichzeitigen Nachrichtenversorgung der Medien zu erfüllen, muss eine Agentur, die über das Internet einige Hundert Kunden beliefert, notwendigerweise über einen Breitbandanschluss von einigen 100 Mb/s verfügen.

Was die Kriterien Schnelligkeit, Gleichzeitigkeit und Ausfallsicherheit betrifft, ist es somit möglich, über das Internet eine zur Satellitenübertragung vergleichbar gute Versorgung der Kunden zu erreichen. Darüber hinaus bilden beide Übertragungswege auch eine sinnvolle Ergänzung zueinander. Wurde oben bereits erwähnt, dass Satellitenfunk im Katastrophenschutz als alternative Kommunikationsverbindung im Krisenfall eine wichtige Rolle spielt, so nutzt umgekehrt die Satellitenkommunikation das Internet als redundanten Übertragungsweg, im Falle, dass durch lokale Witterungsbedingungen (z. B. starke Gewitter, die zu einer elektrostatischen Aufladung der Atmosphäre führen) einzelne Sende- oder Empfangsanlagen temporär nicht einsatzfähig sind. Über einen Internet-Back-Channel haben dann die Kunden über einen zentralen Server Zugriff auf die Nachrichten.

Der wesentliche Sicherheitsaspekt, dem bei der Internetübertragung besondere Aufmerksamkeit zukommen muss, ist die Authentizität der Nachrichten: Im Gegensatz zur Satellitenkommunikation ist in terrestrischen Netzen ein direkter Eingriff in den Datenstrom prinzipiell auf der gesamten Übertragungsstrecke mit relativ geringem apparativem Aufwand möglich. Es ist daher zwingend notwendig, dass der Empfänger einer Nachricht deren Absender jederzeit verlässlich identifizieren kann. Weiterhin muss er überprüfen können, ob die Nachricht während der Übertragung verändert wurde.

Beide Sicherheitsanforderungen lassen sich erfüllen, wenn alle übertragenen Nachrichten mit einer Signatur versehen sind, deren Gültigkeit der Empfänger auf Grundlage einer Public-Key-Infrastruktur (PKI) überprüfen kann. Das bedeutet, dass

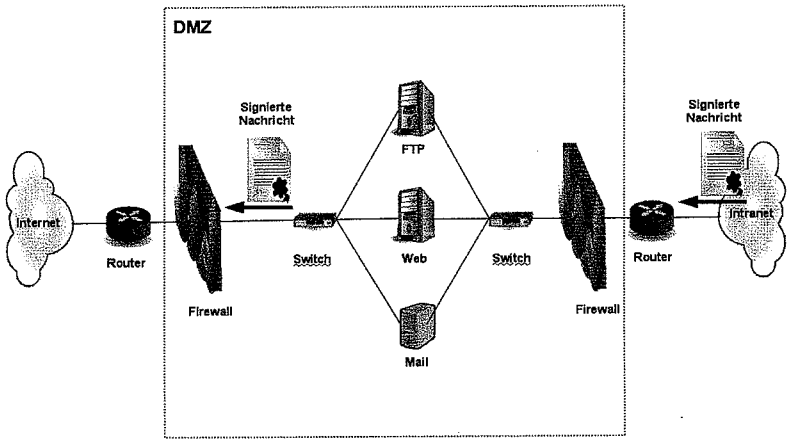

Abbildung 2: Signierte Nachrichten werden aus dem Intranet der Agentur auf Servern in einer DMZ abgelegt – dort können sie von den Kunden per HTTP- oder FTP-Pull über das Internet abgeholt werden oder sie werden ihnen per E-Mail zugestellt.

das Zertifikat von einer Certification-Authority (CA) ausgegeben wurde, welche über öffentlich erreichbare Kommunikationsverbindungen (z. B. Internet) die Zuordnung zu einer identifizierten Person bestätigt. Die Nachricht lediglich mit einer Prüfsumme (z. B. MD5-Hash) zu versehen, reicht nicht aus, da diese zum einen keine eindeutige Identifizierung des Absenders erlaubt und zum anderen von einem Angreifer zusammen mit der Nachricht selbst gefälscht worden sein könnte.

Die Übertragung zwischen der Agentur und den Kunden sollte natürlich so erfolgen, dass nicht nur die Authentizität der Nachrichten, sondern auch die Sicherheit der internen Netze beider Partner gewährleistet ist. Entsprechende Sorgfalt ist daher auf die Konzeption und Umsetzung der Verfahren zu verwenden, mit denen die Daten für die Kunden bereitgestellt werden. Eine mögliche Serverarchitektur hierzu zeigt Abbildung 2: Die Informationsserver mit den (signierten) Daten stehen dabei in einer „demilitarisierten Zone" (DMZ) zwischen zwei Firewalls, welche den Zugriffe sowohl aus dem Internet (Nachrichten-Download durch die Kunden) als auch aus dem internen Netz der Agentur (Upload der Nachrichten auf die Server) überwachen. Derzeit am häufigsten angeboten werden der Web- und FTP-Download sowie die Zustellung per E-Mail. Hinsichtlich der Einzelheiten zur sicheren Konfiguration solcher Dienste sei auf die Grundschutzkataloge und die ISI-Reihe (ISI = Internet-Sicherheit) verwiesen, die auf der BSI-Homepage (www.bsi.bund.de) zum kostenlosen Download bereitstehen.

An dieser Stelle sei daher lediglich auf zwei Sicherheitsaspekte hingewiesen: Zum Schutz der Kunden sollten außer bei E-Mail keine Push-Dienste angeboten werden. Die Verbindung zu einem Web- oder FTP-Server sollte immer von der Client-Seite aus initiiert werden (goldene Regel aus Sicht des Kundennetzes: „Verbindungsaufbau nur von innen nach außen"). Ist zum Zugriff auf die Informationsdienste eine Zugangskennung notwendig, sollte statt der Protokolle http und ftp die mit SSL-Verschlüsselung arbeitenden Varianten https und ftps verwendet werden. Auf diese Weise werden der User-Name und das Passwort verschlüsselt übertragen und können von einem Angreifer nicht missbraucht werden.

Fazit

Zur Verbreitung von Agenturnachrichten haben sich mit der Satellitenkommunikation und dem Internet in den letzten drei Jahrzehnten zwei alternative Übertragungswege herausgebildet. Bietet die Satellitenkommunikation systembedingt Vorteile bei der Sicherheit und Verfügbarkeit, so stehen diesen ein hoher apparativer Aufwand und die damit verbundenen Kosten gegenüber. Mit dem stetig wachsenden Angebot an Breitbandverbindungen lässt sich eine nahezu gleichzeitige Versorgung aller Agenturkunden auch über das Internet erreichen. Da bei terrestrischen Netzen prinzipiell ein höheres Bedrohungspotenzial besteht, müssen verstärkte Sicherheitsmaßnahmen sowohl zum Schutz der internen Netze der Agenturen und ihrer Kunden als auch zur Gewährleistung der Authentizität der übertragenen Nachrichten getroffen werden. Letzteres lässt sich insbesondere durch die Verwendung PKI-basierter Signaturen erreichen. ■

kurz notiert

Anti-Botnet-Beratungszentrum gestartet

Mitte September hat das Anti-Botnet-Beratungszentrum seine Tätigkeit als Anlaufstelle für Internetnutzer aufgenommen, deren Computer mit einem Botnetz-Schadprogramm infiziert ist. Das Projekt wird vom Bundesamt für Sicherheit in der Informationstechnik (BSI) technisch unterstützt und vom Bundesministerium des Innern (BMI) durch eine Anschubfinanzierung aus Mitteln des IT-Investitionsprogramms gefördert – federführender Träger ist der eco – Verband der deutschen Internetwirtschaft e. V.

Anlässlich des operativen Starts erklärte BSI-Vizepräsident Horst Flätgen: „Botnetze sind aktuell eine der größten Gefährdungen für das Internet und die daran angeschlossenen Infrastrukturen. Um sich gegen Botnetze zu wappnen, brauchen die Bürger vor allem Aufklärung, Beratung und aktive Unterstützung. Das Anti-Botnet-Beratungszentrum leistet genau dies und wird das Internet ein Stück sicherer machen."

Im Rahmen des Projekts informieren teilnehmende Internetserviceprovider betroffene Kunden über eine mögliche Infektion ihres Rechners mit einem Schadprogramm. Dabei weisen sie auf Informationen und Tools zur selbstständigen Überprüfung und Säuberung des PCs hin, die über die Website www.botfrei.de zur Verfügung stehen. Sollten diese Maßnahmen nicht ausreichen (etwa bei sehr stark infizierten Rechnern), erhält der Anwender über seinen Internetserviceprovider die Möglichkeit, eine telefonische Beratungshotline zu nutzen. ■

Weitere Informationen zum Thema Botnetze sind auf den Webseiten des BSI (vor allem www.bsi-fuer-buerger.de) sowie des Anti-Botnet-Beratungszentrums abrufbar.