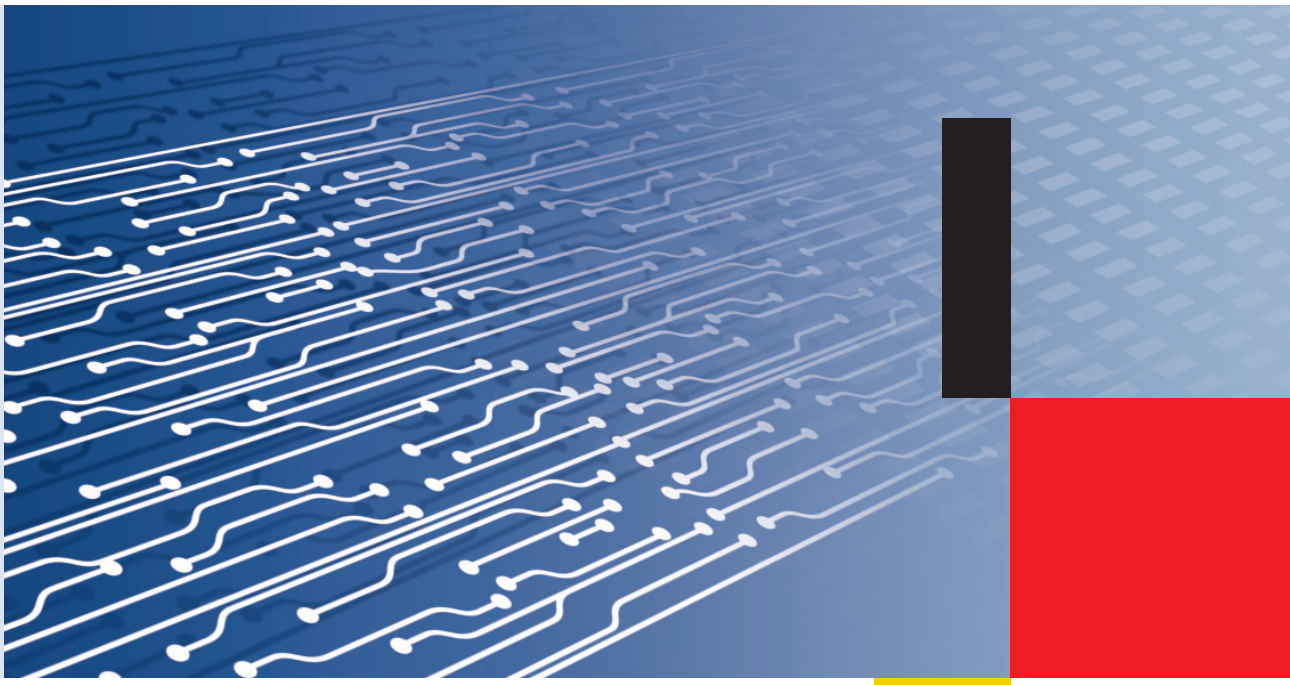
Bundesamt
für Sicherheit in der
Informationstechnik

Die Lage der IT-Sicherheit in Deutschland 2007



Bundesamt für Sicherheit in der Informationstechnik
www.bsi.bund.de

Inhaltsverzeichnis

Abbildungsverzeichnis

Vorwort

1 Vorwort

Die Bedrohungen der Informationstechnik (IT) sind seit der Veröffentlichung des ersten Lageberichts zur IT-Sicherheit in Deutschland im Jahr 2005 unvermindert angestiegen. Die verstärkte berufliche und private Abhängigkeit von moderner Kommunikationstechnik bringt eine Erhöhung der IT-Risiken mit sich.

Der vorliegende Bericht stellt die aktuelle Lage der IT-Sicherheit in Deutschland dar. Er gibt einen Überblick über gegenwärtige und künftige Risiken, Herausforderungen und Trends und erlaubt ihre Einordnung und Bewertung. Unsere Gesellschaft benötigt zuverlässige Informationen. Und sie braucht sichere Kommunikationswege, damit die Informationen ihre Adressaten auch erreichen. Die ansteigende Bedrohung durch IT-Schädlinge, der Trend zur Kommerzialisierung und Professionalisierung der Internetkriminalität, das geringe Schutzniveau vieler IT-Systeme – all das sind Warnhinweise, die eine ganzheitliche und nachhaltige IT-Sicherheitsstrategie erforderlich machen.

Inzwischen leisten fast 500 Mitarbeiterinnen und Mitarbeiter im BSI ihren Beitrag zur Inneren Sicherheit Deutschlands. Mit dieser Konzentration von Expertenwissen zum Thema IT-Sicherheit verfügt die Bundesrepublik über eine europaweit einmalige Institution. Als nationale IT-Sicherheitsbehörde ist das BSI auch koordinierend für die Umsetzung des Nationalen Plans zum Schutz der Informationsinfrastrukturen verantwortlich. Eine dauerhafte Verbesserung des IT-Sicherheitsniveaus kann allerdings nicht alleine durch Experten erzielt werden – alle gesellschaftlichen Gruppen müssen dazu ihren Beitrag leisten.

Mai 2007

Dr. Udo Helmbrecht

Präsident des BSI

Einleitung

2 Einleitung

Die Vorteile neuer Kommunikationswege für die Informationsgesellschaft liegen auf der Hand: erweiterte Bildungsmöglichkeiten, allgemeiner Zugang zu Informationen über das Internet und dadurch eine Effizienzsteigerung in vielen Bereichen. Wie fast jede bedeutende Entwicklung birgt aber auch die fortschreitende Vernetzung neue Herausforderungen. Ob im privaten oder geschäftlichen Umfeld: IT-Systeme sind verwundbar, durch Hacker ebenso wie durch Computerviren und -würmer.

IT-Sicherheit ist daher ein Gebot der Stunde. Aber wann gilt die IT-Lage eigentlich als sicher? Aus Sicht des BSI erst dann, wenn Vertraulichkeit, Integrität und Verfügbarkeit von Informationen wie von Informationstechnik gleichermaßen durch angemessene Maßnahmen geschützt sind.

Die ersten Meldungen über PC-Viren liegen bereits zwanzig Jahre zurück. Damals wurde der Schädling per Floppy-Disk von einem Computer auf den anderen übertragen. In der heutigen vernetzten Welt hingegen verbreiten sich Viren und Würmer innerhalb von Sekunden weltweit und befallen ungeschützte PCs. Zahlreiche neue Schädlingsvarianten werden jeden Tag registriert. „Zero Day Exploits“ nutzen Sicherheitslücken immer öfter unmittelbar nach ihrem Bekanntwerden aus. Der Anteil an Spam-Nachrichten am gesamten E-Mail-Verkehr steigt extrem an und die zunehmenden Phishing-Attacken gefährden das Vertrauen in die Sicherheit des Internets.

Seit dem Auftauchen des ersten PC-Virus hat sich nicht nur die Zahl der Attacken, sondern auch die Motivation der Angreifer erheblich verändert: Die durch „sportlichen“ Ehrgeiz motivierten individuellen Computerhacker sind in den meisten Fällen der professionalisierten Kriminalität gewichen. Zudem werden die Angriffe zielgerichteter und raffinierter. Kriminelle „Geschäftsmodelle“ wie Identitätsdiebstahl und Erpressung werden durch die zunehmende Verlagerung alltäglicher Aktivitäten wie Einkäufe oder Bankgeschäfte ins Internet begünstigt. Virtuelle Identitäten ermöglichen es Kriminellen, weitgehend anonym aufzutreten. Dabei sind vor allem die Systeme der Privatanwender ein beliebtes Angriffsziel.

Im täglichen Umfeld ist auch der (Un-)Sicherheitsfaktor Mensch nicht zu vernachlässigen. Nicht immer wird dabei vorsätzlich gehandelt: So können Opfer von Computerschädlingen durch die unwissentliche Zugehörigkeit zu einem Bot-Netz ungewollt zu Tätern werden. Und Arbeitnehmer können ihren Unternehmen durch gedankenloses Verhalten mitunter beträchtlichen Schaden zufügen.

Im zweiten Bericht zur Lage der IT-Sicherheit in Deutschland werden aktuelle und vorhersehbare Bedrohungen beschrieben, die durch technische Sicherheitslücken und ihre Ausnutzung entstehen. Darüber hinaus werden aber auch Chancen und Risiken beim Einsatz innovativer Technologien präsentiert sowie Trends aus den Bereichen Wirtschaft und Gesellschaft, Technik und Recht vorgestellt. Der Bericht vermittelt zudem einen Überblick über den Umgang verschiedener gesellschaftlicher Gruppen mit der Informationstechnik und die Aktivitäten und Hilfestellungen, die das BSI diesen Zielgruppen an die Hand gibt.

Untermauert werden die dargestellten Informationen durch Erkenntnisse aus eigenen Erhebungen des BSI, aus Fachkontakten und aus Studien verschiedener IT-Dienstleister.

IT-Sicherheitsbewusstsein und IT-Sicherheitskompetenz in der Gesellschaft

3 IT-Sicherheitsbewusstsein und IT-Sicherheitskompetenz in der Gesellschaft

Die neuen Kommunikationsformen der Informationstechnologie erfreuen sich in unserer Gesellschaft immer größerer Beliebtheit, gleichzeitig steigen die Gefahren etwa durch Trojanische Pferde oder Bot-Netze. Dennoch ist das Bewusstsein, wie wichtig IT-Sicherheit ist, über die unterschiedlichen gesellschaftlichen Gruppen hinweg nach wie vor wenig ausgebildet. Immerhin beginnen sich in einigen Bereichen gegenläufige Tendenzen abzuzeichnen – ein wichtiger Schritt in die richtige Richtung. Denn durch Gefahrenbewusstsein steigt die Motivation, sich die nötigen Kompetenzen anzueignen und empfohlene Sicherheitsmaßnahmen ernsthaft umzusetzen. Wer den Sinn hinter diesen Schritten hingegen nicht erkennt, neigt erfahrungsgemäß zu nachlässiger Umsetzung oder sucht gar nach Wegen, sie zu umgehen.

3.1 Bürger

Über 60 Prozent der Haushalte in der Bundesrepublik besitzen einen Internetzugang.[1] Mit der konstant ansteigenden Zahl der Internetnutzer ist offenbar auch das Bewusstsein dafür gestiegen, dass der eigene PC geschützt werden muss. Das Wissen über Angriffsmöglichkeiten war bei den meisten Nutzern zwar auch schon früher vorhanden, doch kümmerten sich die wenigsten aktiv um einen ausreichenden Schutz ihres Computers.[2] Hier ist ein positiver Trend zu verzeichnen: So ist etwa nach BSI-Erhebungen der Anteil der Privatnutzer, die einen Virenscanner einsetzen, innerhalb von drei Jahren um 14 Prozentpunkte auf insgesamt 90 Prozent gestiegen.

Ein wesentlicher Grund dafür besteht darin, dass mittlerweile vier von fünf Nutzern auf die eine oder andere Weise mit Computergefährdungen in Kontakt gekommen sind. Viren und Würmer sind dabei die Spitzenreiter – dicht gefolgt von unerwünschten E-Mails und Trojanischen Pferden.[3] Zudem zeigen Befragungen, dass die Bedeutung von PC und Laptop für die Bürger steigt. Wer zunehmend Aktivitäten wie Bankgeschäfte und Einkaufen online erledigt, ist damit auch stärker von der Verfügbarkeit des Internets abhängig.

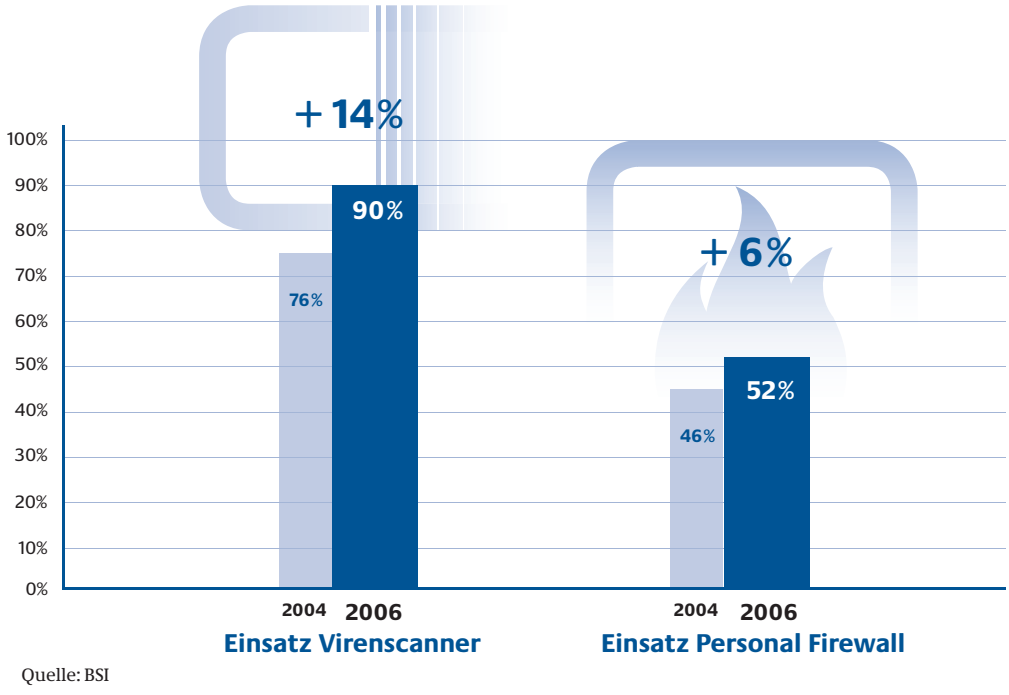


Abbildung 1: Einsatz von Virenscanner und Firewall auf den PCs deutscher Internetnutzer [3]

Darüber hinaus ist das Thema IT-Sicherheit zunehmend in den Medien präsent. Und nicht zuletzt betreiben Institutionen wie das BSI verstärkt Aufklärungsarbeit.

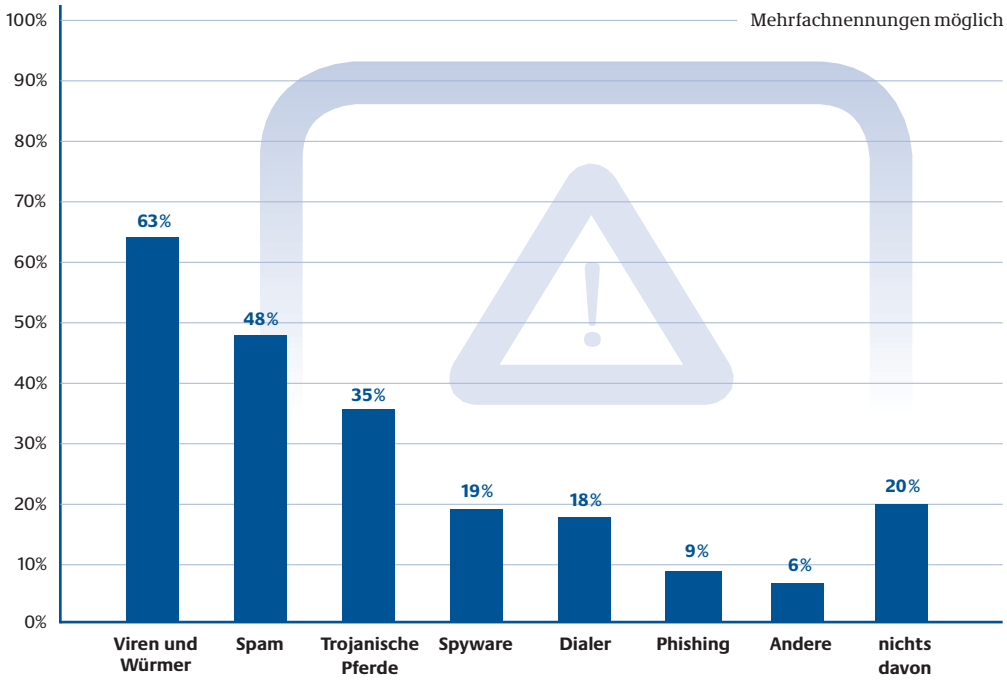
All diese Faktoren haben auch dazu geführt, dass Privatnutzer ihre IT-Kompetenz realistischer einschätzen: Im Jahre 2004 gaben noch 46 Prozent der Befragten an, sich sehr gut oder zumindest gut mit IT-Sicherheit auszukennen. 2006 sind dies nach Erkenntnissen des BSI nur noch knapp 17 Prozent.

Immerhin ist vielen Bürgern bekannt, dass Werkzeuge wie Virenscanner und Firewall einen wichtigen Beitrag zur IT-Sicherheit leisten. Die Entwicklung beim Einsatz dieser Produkte ist jedenfalls positiv. Rund die Hälfte der befragten Nutzer äußern sogar die Bereitschaft, mehr Geld für IT-Sicherheitsprodukte zu bezahlen – vorausgesetzt, deren Qualität wird durch eine neutrale Stelle bestätigt.

Einerseits ist zwar die Bereitschaft zu stärkeren Investitionen in IT-Sicherheit vorhanden, andererseits werden selbst grundlegende Warnhinweise nicht

berücksichtigt: So melden sich beispielsweise mehr als die Hälfte der befragten Nutzer nicht wie von Sicherheitsexperten empfohlen mit beschränkten Benutzerrechten, sondern mit uneingeschränkten Administratorenrechten an ihrem Computer an. Eine Konsequenz daraus: Infektionen mit Computerschädlingen, die etwa beim Surfen im Internet sehr schnell erfolgen, können wesentlich schwerwiegendere Folgen nach sich ziehen.

Persönliche Erfahrung mit Online-Bedrohungen



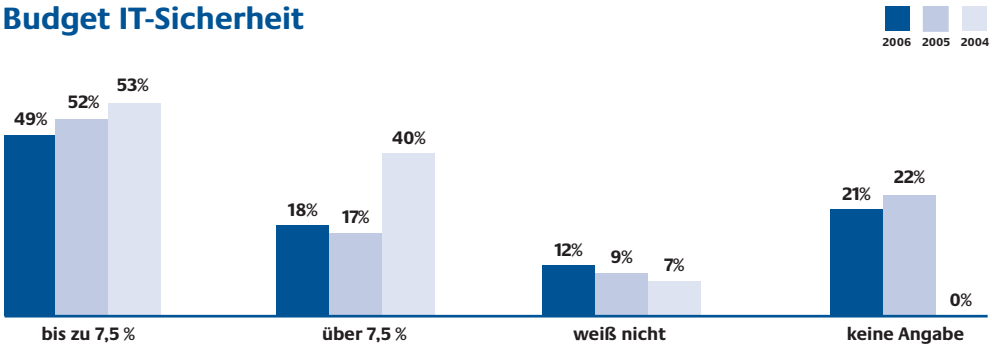
Quelle: BSI

Abbildung 2: Internetgefährdungen, von denen Bürger bereits betroffen waren [3]

Zusammenfassend ergibt sich ein zwiespältiges Bild: Das Bewusstsein für IT-Sicherheit ist vorhanden. Andererseits besteht auch eine Tendenz, die Lösung der Probleme vor allem an Internetanbieter und die Hersteller von IT-Sicherheitslösungen delegieren zu wollen. Dies ist zweifelsohne wichtig, denn die IT-Sicherheit muss verstärkt als eine notwendige Produkteigenschaft von Systemen und Diensten eingefordert werden. Jede technische Maßnahme zur Absicherung eines IT-Systems ist jedoch nur die Hälfte wert, wenn der Mensch, der es bedient, nicht sensibel ist für IT-Sicherheit, entsprechende IT-Sicherheitsmaßnahmen nicht akzeptiert und IT-Sicherheit selbst nicht aktiv betreibt.

3.2 Wirtschaft

In Umfragen bezeichneten IT-Verantwortliche in der Wirtschaft auch 2006 das Thema IT-Sicherheit als absolut vorrangig. Die Budgets sprechen allerdings eine andere Sprache: Nur knapp ein Fünftel investiert mehr als 7,5 Prozent des gesamten IT-Budgets in IT-Sicherheit – im Jahr 2004 waren das mit 40 Prozent der Befragten noch mehr als doppelt so viele.[4]



Quelle: Capgemini

Abbildung 3: Anteil der jährlichen IT-Sicherheitsausgaben am gesamten IT-Budget (in Prozent) [4]

Im Branchenvergleich zeigt sich, dass im Finanzsektor die Sicherheitsrisiken noch am ehesten erkannt werden.

Eine Ursache für die mangelnde Investition in IT-Sicherheit ist auf der Ebene der Geschäftsleitung und des Managements anzusiedeln: Mehr als die Hälfte der Befragten schätzt das Bedrohungsrisiko für das eigene Unternehmen als gering ein. Sicherheitsrisiken werden darüber hinaus eher als technische und nicht als betriebswirtschaftlich relevante Probleme gesehen. Hinsichtlich Prävention und Umgang mit IT-Sicherheitsrisiken wird also in Führungskreisen oft nicht ausreichend verantwortungsbewusst agiert. Richtlinien zur Informationssicherheit existieren nur in jedem fünften deutschen Unternehmen. Selbst dort, wo es Regeln gibt, sind wiederum nur knapp zwei Drittel der betreffenden Mitarbeiter auch damit vertraut.[5]

Dabei können Versäumnisse schwerwiegende Folgen haben. Abgesehen von den Kosten für IT-Zwischenfälle und einem damit verbundenen möglichen Imageverlust nimmt inzwischen auch die Frage der persönlichen Haftung

eine stärkere Bedeutung ein. Insbesondere durch das Gesetz zur Kontrolle und Transparenz im Unternehmensbereich (KonTraG) wurden die einschlägigen Gesetze des Gesellschaftsrechts um Regelungen ergänzt, die es erlauben, Schadensersatzansprüche des Unternehmens gegen Vorstände oder Geschäftsführer geltend zu machen.

Der Faktor Mensch – also der Irrtum und die Nachlässigkeit eigener Mitarbeiter – stellt nach einer Umfrage der Zeitschrift für Informations-Sicherheit „kes“ für die Mehrheit der Befragten die eindeutig größte Gefahr für die IT-Sicherheit des eigenen Unternehmens dar. Erst an zweiter Stelle der Gefahren folgen im Jahr 2006 Schadprogramme wie Trojanische Pferde, Viren und Würmer. Auch wenn es in diesem Zeitraum weniger dramatische Fälle in diesem Bereich gab, stellt die Verbreitung von Schadprogrammen weiterhin eine gefährliche Bedrohung dar. In diesem Gefahrenbereich erwarten IT-Verantwortliche auch für die Zukunft das stärkste Wachstum.[6]

Gefahrenbereich	Bedeutung heute Rang	Prognose Rang	Schäden Rang	Schäden ja, bei
Irrtum und Nachlässigkeit eigener Mitarbeiter	1	2	1	49%
Malware (Viren, Würmer, Trojanische Pferde)	2	1	4	35%
Software-Mängel/-Defekte	3	5	2	46%
Hardware-Mängel/-Defekte	4	6	3	45%
unbefugte Kenntnissnahme, Informationsdiebstahl, Wirtschaftsspionage	5	3	7	12%
unbeabsichtigte Fehler von Externen	6	7	5	30%
Hacking (Vandalismus, Probing, Missbrauch, ...)	7	4	8	12%
Mängel der Dokumentation	8	9	6	20%
Manipulation zum Zweck der Bereicherung	9	8	10	11%
höhere Gewalt (Feuer, Wasser, ...)	10	11	9	12%
Sabotage (inkl. DoS)	11	10	11	10%
Sonstiges	12	12	12	3%

Quelle: kes

Abbildung 4: Bedeutung der verschiedenen Gefahrenbereiche für deutsche Unternehmen [6]

Die Gefährdungen, die von drahtlosen Übertragungstechnologien wie WLAN und dem Datenaustausch über mobile Geräte wie Notebooks oder PDAs ausgehen, werden bisher nur eingeschränkt wahrgenommen. Obwohl diese Technologien bereits aktiv genutzt werden, planen nur 19,8 Prozent der Unternehmen Maßnahmen zum verbesserten Schutz vor den damit verbundenen Risiken.[5]

Kritische Infrastrukturen (KRITIS)

Als „kritisch" werden jene Infrastrukturen bezeichnet, die für das Gemeinwesen lebensnotwendige Dienstleistungen wie Telekommunikation oder Stromversorgung bereitstellen. In Folge der Verabschiedung des Nationalen Plans zum Schutz der Informationsinfrastrukturen (NPSI) durch das Bundeskabinett im Jahr 2005 wird mit den Betreibern Kritischer Infrastrukturen der so genannte Umsetzungsplan KRITIS (UP KRITIS) erstellt. Er soll zur weiteren Verbesserung des IT-Sicherheitsniveaus speziell in diesen sensiblen Bereichen beitragen.

Die im Rahmen der Erstellung des UP KRITIS durchgeführte Bestandsaufnahme zeigt bereits deutlich, dass sich die Betreiber Kritischer Infrastrukturen der Risiken des IT-Einsatzes durchaus bewusst sind und auch entsprechend handeln. IT-Sicherheit wird in diesen Bereichen bereits als Prozess verstanden, der sich von der Managementebene bis zur Ebene der Umsetzung und der Kontrolle einzelner Maßnahmen durchzieht. Auch eine kontinuierliche Anpassung an die aktuellen Erfordernisse ist hier die Regel.

Weniger einheitlich stellt sich das Bild dar, wenn man die einzelnen „kritischen" Branchen vergleicht: Unternehmensübergreifende Kooperationen zur Minimierung von Störungsfolgen auf das Gemeinwesen sind hier sehr unterschiedlich ausgeprägt. Während in manchen Bereichen bereits durchaus eng zusammengearbeitet wird, existieren in anderen nur zaghafte Ansätze.

3.3 Verwaltung

Die Besonderheit der öffentlichen Verwaltung besteht darin, dass sie eine Doppelrolle einnimmt: Einerseits ist auch die Verwaltung in steigendem Maße bei der Wahrnehmung ihrer Aufgaben vom IT-Einsatz abhängig und das Erreichen der Behördenziele an einen sicheren IT-Einsatz gebunden. Sie steht andererseits als Verwalter von Bürger-Identitäten und als Anbieter vielfältiger elektronischer Dienste für Bürger, Wirtschaft und Staat in der Verantwortung.

Im „Bericht zur Lage der IT-Sicherheit in Deutschland 2005“ wurden im Bereich der Verwaltung ähnliche Defizite festgestellt wie bei den Unternehmen. Kritikpunkte waren damals vor allem die mangelnde Sensibilisierung der Entscheidungsträger und das Fehlen von ausreichend qualifiziertem Fachpersonal. Vollständig beseitigt werden konnten diese Defizite innerhalb von zwei Jahren noch nicht, jedoch wurden in vielen Bereichen konkrete Maßnahmen implementiert, die zu einer deutlichen Verbesserung der Situation beigetragen haben. Hierzu zählen Schulungen, der Einsatz von IT-Sicherheitsbeauftragten und die Erstellung von Sicherheitsrichtlinien.

Für den Bereich der Bundesverwaltung wird mit dem Umsetzungsplan Bund (UP Bund) erstmals eine zwischen sämtlichen Bundesressorts abgestimmte IT-Sicherheitsleitlinie für die Bundesverwaltung erstellt.

Auch die Herausforderungen an die öffentlichen Verwaltungen als Verwalter und Hüter der elektronischen Identitäten seiner Bürger gehen in eine neue Dimension. Ob Reisepass, Personalausweis oder Gesundheitskarte – der daraus resultierenden Verantwortung ist sich die Verwaltung bewusst und kommt dieser mit umfangreichen Sicherheitskonzepten nach.

Schwachstellen und Bedrohungen von IT-Systemen

4 Schwachstellen und Bedrohungen von IT-Systemen

4.1 Sicherheitslücken

In komplexen Produkten wie Software kommen regelmäßig Fehler vor. Dadurch entstehen Sicherheitslücken, die von Angreifern mit so genannten Exploits ausgenutzt werden können. Es ist ein Qualitätsmerkmal von Software, wie schnell Hersteller auf solche Lücken reagieren und Sicherheitsupdates veröffentlichen. Nach wie vor werden diese Updates oft erst mit erheblichem Zeitverzug zur Verfügung gestellt, da aufwändige Kompatibilitätstests erforderlich sind. Manchmal kommt es auch vor, dass die Updates fehlerhaft sind, die Schwachstelle nicht vollständig beseitigen oder gar selbst neue Sicherheitslücken verursachen. Auch wenn Updates verfügbar sind, werden diese aufgrund von Unwissen, Nachlässigkeit oder Zeitknappheit der Nutzer oft nicht zeitnah installiert.

7.247 neue Schwachstellen entdeckte ein Sicherheitsunternehmen im Jahr 2006 – ein Anstieg von 40 Prozent im Vergleich zum Vorjahr. Auch der prozentuale Anteil jener Sicherheitslücken, die von Angreifern für den Zugriff auf ein verwundbares System ausgenutzt werden können, erhöhte sich. 52,5 Prozent der im Jahre 2006 analysierten Schwachstellen eigneten sich dafür, Benutzer- oder sogar Administratorrechte zu erlangen. Ende des Jahres 2005 lag dieser Anteil noch bei 43 Prozent.[7]

Der Zeitraum zwischen Bekanntwerden einer neuen Schwachstelle und der Veröffentlichung eines Exploits ist oft zu kurz, um notwendige Programmupdates zur Verfügung zu stellen oder andere Schutzmaßnahmen zu entwickeln. Durchschnittlich benötigen Angreifer nur drei Tage, um einen Exploit zur Ausnutzung der Schwachstelle zu schreiben. Vor zwei Jahren waren es noch 6,4 Tage.[2] Besonders schnell arbeiten die Hacker bei Schwachstellen in Webbrowsern: Hier steht durchschnittlich bereits nach einem Tag ein Exploit zur Verfügung.[8] Und auch die Zahl der so genannten Zero-Day-Angriffe, die eine öffentlich gemachte Sicherheitslücke bereits am gleichen Tag ausnutzen, steigt an. In 44 Prozent der im Jahr 2006 veröffentlichten Informationen zu neuen Sicherheitslücken waren bereits Beispielcodes zu deren Ausnutzung enthalten. Im Jahr zuvor lag dieser Anteil bei lediglich 13 Prozent.[7] Eine Vielzahl von

Exploits, mit denen Angreifer die Kontrolle über ein System erlangen können, sind darüber hinaus im Internet frei verfügbar. Immer öfter werden auch Schwachstellen ausgenutzt, die bislang öffentlich nicht bekannt sind. Eine mögliche Erklärung für diese rasante Beschleunigung könnte darin liegen, dass Cyberkriminalität äußerst lukrativ geworden ist. Für Täter, die sich im Umfeld der organisierten Kriminalität oder der Wirtschaftsspionage bewegen, lohnt es sich immer mehr, Geld in die Entwicklung von Exploits und das Aufspüren neuer Sicherheitslücken zu investieren.

4.2 Schadprogramme

Computerschadprogramme stellen die häufigste Angriffsform gegen IT-Systeme dar. Die starke Verbreitung von Standardsoftware und so genannte Monokulturen bei Betriebssystemen bieten bei Bekanntwerden neuer Schwachstellen eine große Angriffsfläche. Die Autoren von Schadprogrammen zielen daher bevorzugt auf Sicherheitslücken in Standardapplikationen wie Office-Anwendungen oder Webbrowsern. Opfer von Infektionen sind in erster Linie die Rechner ahnungsloser Nutzer im privaten und beruflichen Umfeld. Die Programme werden meistens über E-Mail-Anhänge oder präparierte Webseiten verbreitet. Auch Datenträger können als Übertragungsweg genutzt werden. Gefährlich sind dabei nicht nur ausführbare Dateien. Auch an sich unverdächtige Bilddateien oder Dokumente lassen sich zum Angriff missbrauchen, wenn die ausführende Anwendung eine entsprechende Schwachstelle aufweist.

4.2.1 Trojanische Pferde

Trojanische Pferde sind Programme, die ohne Wissen und Einwilligung der Besitzer auf Rechnern aktiv werden und heimlich Schadfunktionen ausführen. Moderne Trojanische Pferde bieten dem Angreifer umfangreiche Kommunikations- und Steuerungsmöglichkeiten sowie eine Vielzahl von Funktionen, die sich beliebig kombinieren lassen: Sie können fremde Rechner vollständig kontrollieren, Daten ausspionieren, Tastatureingaben und Bildschirmausgaben aufzeichnen oder IT-Systeme sabotieren. Zusätzlich besitzen sie hoch entwickelte Tarnfunktionen und laden Updates über das Internet auf die infizierten Rechner herunter.

Konkret werden Trojanische Pferde zum Beispiel für den Aufbau von Bot-Netzen und die Durchführung von Phishing-Angriffen eingesetzt. Auch die Anwendung in der gezielten Spionage verstärkt sich zusehends. Für Behörden und Unternehmen, die auf die Vertraulichkeit ihrer Daten angewiesen sind, hat sich die Bedrohungslage dadurch dramatisch verändert. Schließlich sind die möglichen Schäden durch Spionage vielschichtig und schwerwiegend: Bedrohung der Inneren Sicherheit, wirtschaftliche Verluste, Preisgabe von Verhandlungspositionen oder Kompromittierung von einzelnen Personen oder Institutionen. Auch Erpressungsfälle sind bereits aktenkundig: Die Täter drohen damit, gestohlene Informationen an die Konkurrenz zu verkaufen oder zu veröffentlichen.

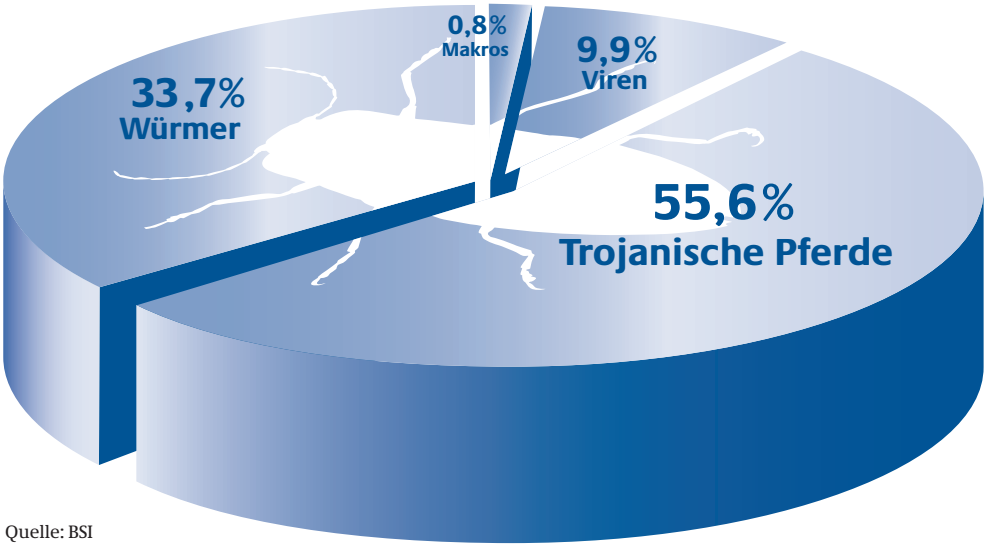
Lange Zeit boten Virenschutzprogramme, Firewalls und regelmäßige Software-Updates einen zuverlässigen Schutz vor Trojanischen Pferden. Die Sicherheitslage hat sich jedoch grundlegend geändert. Bei gezielten Angriffen können moderne Schadprogramme individuell an eine bestimmte Einsatzumgebung angepasst werden, so dass sie von Virenschutzprogrammen nicht erkannt werden. Die Kommunikation mit dem Angreifer erfolgt über das Internet und verwendet Standardprotokolle, die zur Internet- und E-Mail-Nutzung benötigt werden. Firewalls bieten daher in diesen Fällen keinen Schutz.

4.2.2 Viren, Würmer, Spyware

Computerviren stellten bis vor wenigen Jahren die häufigste Form von Schadprogrammen dar. Heute ist die Situation anders: An die Stelle der Viren sind andere Formen von Schadprogrammen getreten: Würmer, Spyware und insbesondere Trojanische Pferde.

In den vergangenen Jahren sorgten Würmer wie Netsky, Bagle oder Sober für großes Aufsehen. Infektionswellen dieser Dimension wurden 2006 nicht registriert. Ein Grund dafür kann darin gesehen werden, dass die Autoren von Schadprogrammen heute nicht mehr darauf abzielen, irreparable Schäden anzurichten oder medienwirksames Aufsehen zu erzeugen. Stattdessen versuchen die Angreifer, durch die Infektionen möglichst viele Systeme ohne Wissen der Nutzer für einen längeren Zeitraum unter ihre Kontrolle zu bringen.

Schädlingsaufkommen 2006



Quelle: BSI

Abbildung 5: Registrierte Schädlinge im Informationsverbund Berlin-Bonn (IVBB) im Jahr 2006 in % [3]

Würmer nutzen zu ihrer Verbreitung hauptsächlich das Transportmedium E-Mail, im letzten Jahr aber auch zunehmend Instant-Messaging. Darüber hinaus werden IT-Systeme immer häufiger auch durch speziell präparierte Webseiten infiziert, die Aktive Inhalte wie JavaScript oder ActiveX enthalten. Es reicht der bloße Besuch einer so manipulierten Seite, um durch Ausnutzung einer Sicherheitslücke im Browser einen PC zu infizieren.

In der Art der Programmierung ist ebenfalls ein neuer Trend zu beobachten: Computerschadprogramme werden von ihren Autoren immer modularer aufgebaut. Dabei treten kleine Programme, so genannte Downloader, in den Vordergrund, die zu bestimmten Zeitpunkten oder auf Anweisung des Angreifers weitere Schadfunktionen aus dem Internet nachladen. Diese Methode ermöglicht dem Angreifer, die Schadprogramme auf den infizierten Systemen durch optimierte Versionen zu ersetzen. Durch die regelmäßige Veränderung der Dateien wird überdies die Erkennung durch Virenschutzprogramme verhindert. Die früher häufig eingesetzten Schadprogramme, die eine Vielzahl von Funktionen in einer einzelnen Datei vereinen, werden hingegen immer seltener.

Spyware stellt weiterhin eine starke Bedrohung dar. Diese Schadsoftware installiert sich ohne Wissen des Benutzers und sammelt Informationen, etwa indem Datenbestände nach Stichworten durchsucht, E-Mails mitgelesen oder Tastatureingaben überwacht werden. Die auf diese Weise ausspionierten Benutzernamen und Kennworte werden dann über das Internet an den Angreifer weitergegeben. Adware, Software mit Werbung, sammelt ebenso wie Spyware Daten und gibt diese weiter. Die gesammelten Informationen dienen dazu, Benutzerprofile zu erstellen, und werden in der Regel für gezielte Werbeeinblendungen verwendet.

4.3 DoS-Angriffe

Ein Denial-of-Service-Angriff (DoS-Angriff) bezeichnet allgemein einen Angriff gegen die Verfügbarkeit eines IT-Systems oder -Dienstes mit dem Ziel, den Zugriff der Nutzer zum Beispiel auf einen Online-Shop zu verhindern. Dazu nutzen Angreifer gezielt Schwachstellen in Betriebssystemen oder Anwendungen aus, um das System oder den Dienst arbeitsunfähig zu machen. Noch weitaus häufiger werden Systeme mit unnützen Datenpaketen überschwemmt, um sie auf diese Weise lahm zu legen. Um die Datenmengen zu erhöhen und die Angriffe damit noch effektiver zu machen, wurden in den letzten Jahren zunehmend verteilte (distributed) Denial-of-Service-Angriffe (DDoS) durchgeführt. Dazu verschaffen sich Angreifer zunächst Ausführungsrechte auf mehreren ungeschützten fremden Computern und installieren dort eine DDoS-Software. Die durch die Angreifer übernommenen Rechner nehmen auf diese Weise ohne Wissen des Computerbesitzers an koordinierten Angriffen teil.

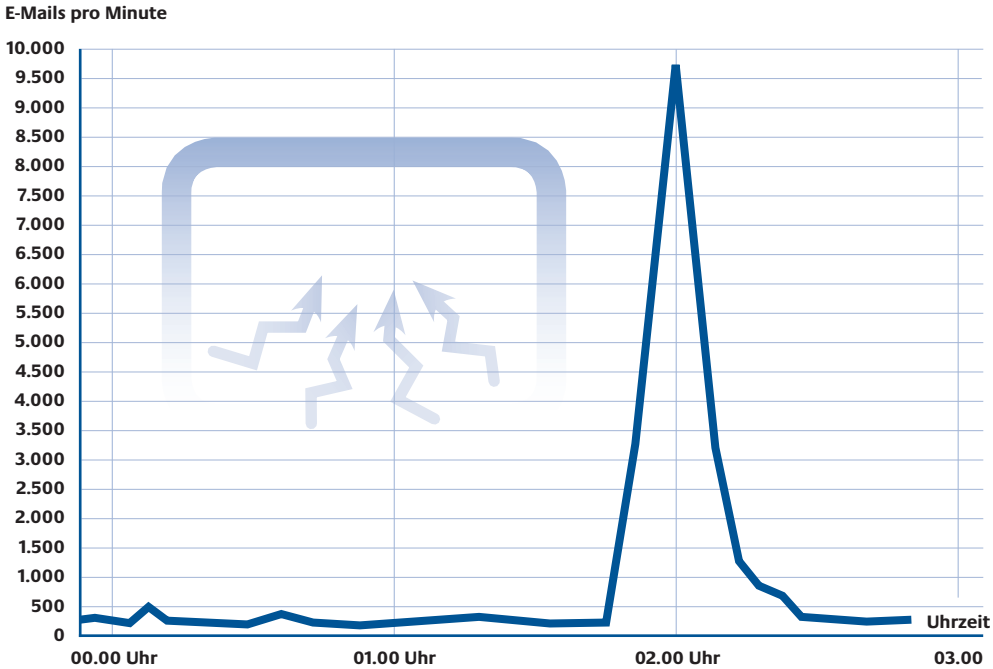
Eine häufige Form dieser Angriffe sind so genannte SYN-Floods. Dabei werden Netzwerk-Verbindungen zum Angriffsziel aufgebaut, deren Initialisierung jedoch nicht abgeschlossen wird. Die große Anzahl solcher „halb offenen“ Verbindungen führt dazu, dass das System keine weiteren regulären Verbindungen mehr annehmen kann. Die Zahl solcher SYN-Flood-Angriffe steigt rasant, wie eine Studie belegt: Demnach wurden im zweiten Halbjahr 2004 durchschnittlich 119 solcher Angriffe pro Tag gezählt, im ersten Halbjahr 2005 bereits 927 – ein Anstieg um 680 Prozent. Im zweiten Halbjahr 2005 wuchs die Anzahl dieser Angriffe erneut um 51 Prozent auf 1.402 täglich. Als Grund für den enormen Zuwachs dieser Angriffe wird die Verbreitung von Bot-Netzen vermutet.[9]

Für den regulären Betrieb von Internetservern stellen DDoS-Angriffe nach wie vor eine ernste Bedrohung dar. Sie lassen sich nicht verhindern, können aber mit zur Verfügung stehenden Maßnahmen zumindest deutlich erschwert werden.

4.4 Unerwünschte E-Mails

Die Kommunikation über E-Mail hat sich zu einer der wichtigsten Anwendungen des Internets entwickelt. Ein Ausfall dieses Dienstes ist für über 80 Prozent der Unternehmen für höchstens einen Tag tolerabel. Unerwünschte Nachrichten, die mittlerweile einen Anteil von rund 80 Prozent des Gesamtaufkommens einnehmen, stellen eine erhebliche Belastung für E-Mail-Server dar.[10]
Im Behördennetz IVBB fielen zum Ende des Jahres 2006 beispielsweise etwa 85 Prozent der E-Mails in diese Kategorie. Zu den Konsequenzen der E-Mail-Flut zählen Arbeitszeitausfälle, eine Überlastung technischer Komponenten und unnötige Kosten für den unerwünschten Datenverkehr.

Spam-Angriff auf einen E-Mail-Server



Quelle: BSI

Abbildung 6: Darstellung eines Denial-of-Service-Angriffs mit unerwünschten E-Mails im August 2006 [3]

Trotz des hohen Aufkommens an unerwünschten E-Mails werden Gegenmaßnahmen in Deutschland immer noch nicht flächendeckend umgesetzt – weder in Unternehmen, noch in der Verwaltung. Der Anteil von Organisationen, die keinen Spam-Filter einsetzen, lag noch 2006 bei etwa zehn Prozent.[5,10] Internet- und E-Mailprovider bieten ihren Kunden häufig Anti-Spam-Dienstleistungen an und verbieten gleichzeitig in ihren Nutzungsbedingungen den Versand von Spam. Trotzdem gaben in einer Anfang 2006 durchgeführten europaweiten Studie dreizehn Prozent der befragten Provider zu, dass sich unter ihren Kunden Spammer befinden.[11]

Die zentralen Schutzmaßnahmen vor unerwünschten E-Mails stellen Wort- und Briefkopf-Analyseverfahren dar. Zudem existieren schwarze und weiße Listen, in denen bekannte Spam-Versender bzw. als sicher geltende Versender aufgelistet sind. Eine weitere Gegenmaßnahme ist das „Greylisting“. Es beruht darauf, dass die oft zur Verbreitung unerwünschter E-Mails benutzten Schadprogramme bestimmte Mechanismen zur Steigerung der Verlässlichkeit der Übertragung von E-Mail nicht beherrschen.

Die Wirksamkeit der Maßnahmen ist jedoch beschränkt, so dass sich trotz der zunehmenden Verfügbarkeit von Anti-Spam-Lösungen nach Erkenntnissen des BSI noch keine wirkliche Entspannung für die Netzbetreiber abzeichnet.

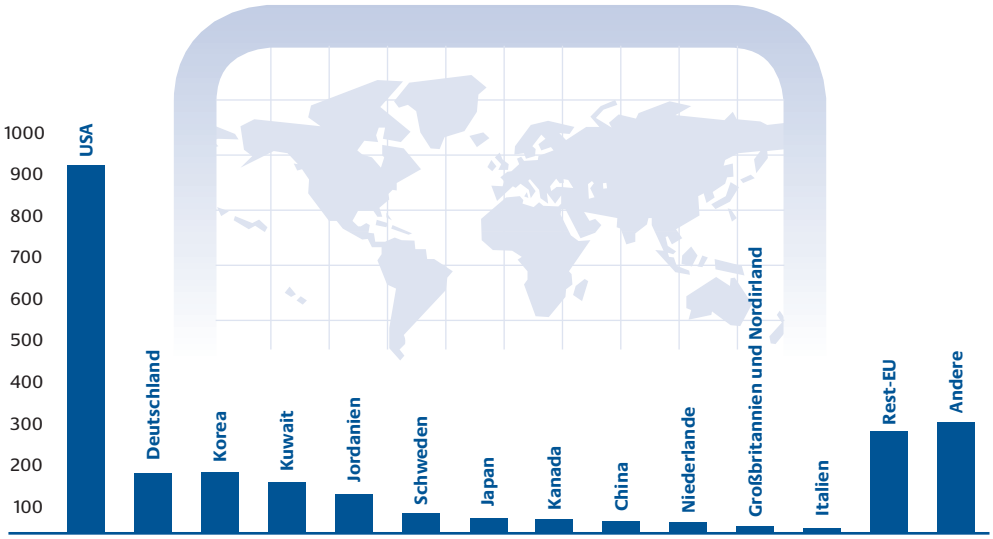
4.5 Bot-Netze

Ein Bot (Kurzform von Robot) ist ein Programm, das ferngesteuert arbeitet. Im Kontext von Computer-Schadprogrammen ist mit Bot ein Programm gemeint, welches einem Angreifer die Fernsteuerung von infizierten Rechnern ermöglicht. Von Bot-Netzen spricht man, wenn viele infizierte PCs per Fernsteuerung zusammengeschlossen und zu bestimmten Aktionen missbraucht werden. Bot-Netze werden zum Beispiel zur Durchführung von DDoS-Angriffen oder zur Versendung von Spam verwendet.

Zur Infektion eines PCs mit einem Bot machen sich Angreifer primär Schwachstellen in Netzwerken zu Nutze. Immer häufiger werden Bot-Programme auch über E-Mail-Anhänge oder präparierte Webseiten auf den PC der Anwender geschleust.

Das zentrale Steuerelement eines Bot-Netzes ist der Command-and-Control-Server (C&C-Server). Die mit einem Bot infizierten Rechner-Systeme bauen eigenständig eine Verbindung zu diesem Server auf und nehmen ihre Anweisungen von dort entgegen. BSI-Erhebungen zeigen, dass die Halbwertzeit der C&C-Server nur bei circa vier Monaten liegt. Die meisten C&C-Server stehen erwartungsgemäß in der „IT-Hochburg“ USA, gleich dahinter folgt jedoch bereits Deutschland. Ein Grund dafür liegt sicherlich in der weiten Verbreitung von Mietservern hierzulande. Die Bundesrepublik ist – ebenso wie alle anderen Industrienationen – aber auch ein populäres Ziel von DDoS-Angriffen.

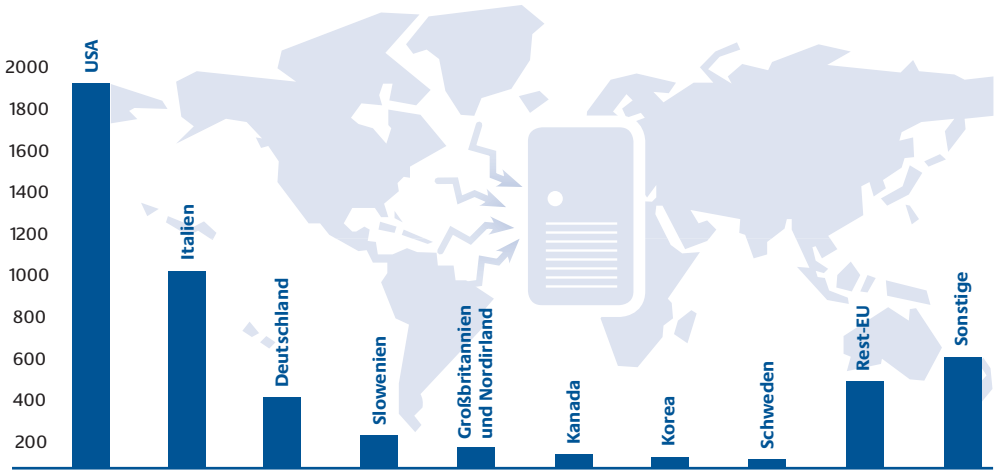
Steuerung von Bot-Netzen



Quelle: BSI

Abbildung 7: Geografische Verteilung der beobachteten Command-and-Control-Server in einem Zeitraum von 12 Monaten [3]

DDoS-Angriffe auf Server



Quelle: BSI

Abbildung 8: Geografische Verteilung von DDos-Angriffen innerhalb eines zeitlich begrenzten Beobachtungsprojekts [3]

Die Anzahl der Computer, die zu jeweils einem Bot-Netz zusammen geschlossen sind, hat sich in der letzten Zeit merklich verringert. Dieser auf den ersten Blick positiv anmutende Trend hat jedoch einen Haken: Die Zahl der kleineren und damit wendigeren Bot-Netze ist gestiegen. Der Vorteil für die Betreiber: Durch die erhöhte Flexibilität sind die Bot-Netze schwerer zu entdecken und können so einer Zerschlagung viel leichter entgehen.

Die Bedrohung, die von Bot-Netzen ausgeht, ist ungebrochen hoch. Wie auch in anderen Bereichen der IT-Manipulationen sind die Täter zunehmend kriminell motiviert. Ihre „Geschäftsmodelle“ heißen Klickbetrug, Passwort-Spionage mittels Keylogger und Passwort-Sniffer, DDoS-Angriffe gegen Konkurrenten oder Erpressung.

Gegenmaßnahmen zeigen allerdings bereits Wirkung: Die verstärkte Kooperation zwischen Providern, CERTs und IT-Sicherheitsexperten – auch auf internationaler Ebene – trägt dazu bei, dass Bot-Netze schneller aufgedeckt und zerschlagen werden können. Auch verstärkte Maßnahmen zur Aufklärung und Sensibilisierung der Privatanwender haben dazu geführt, dass Firewalls immer konsequenter eingesetzt und Updates regelmäßig installiert werden. Immer mehr Bürger erkennen wohl auch, dass sie ihr PC als Teil eines Bot-Netzes zu unfreiwilligen Tätern bei schwerwiegenden Delikten wie Wirtschaftsspionage oder Erpressung machen kann.

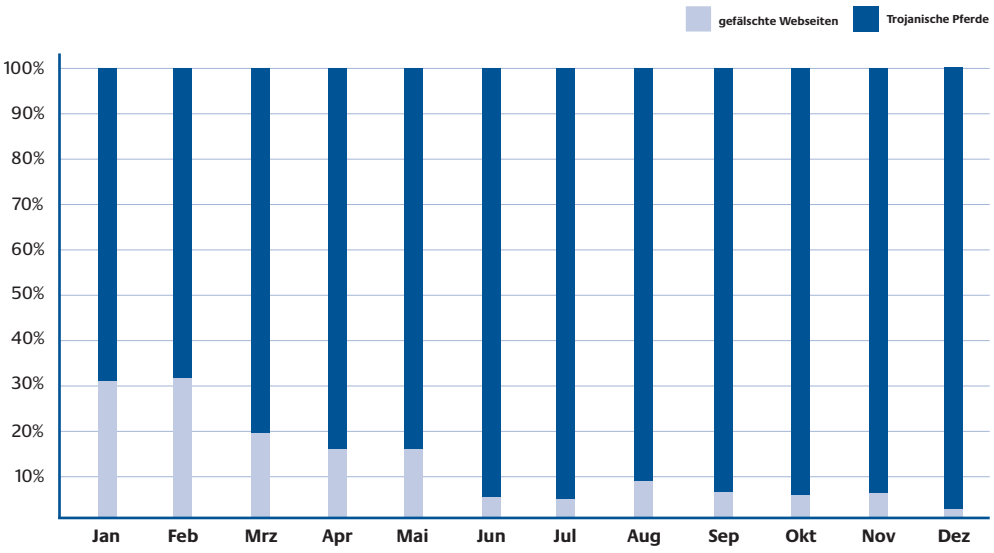
4.6 Phishing und Identitätsdiebstahl

Das Ausspionieren und der Missbrauch vertraulicher Daten in E-Commerce-Infrastrukturen und Online-Bezahlsystemen ist weiterhin stark verbreitet. Die populärste Methode dazu war bisher das Versenden von Phishing-Mails. Dabei werden E-Mails mit falschen Absenderadressen verschickt, deren Aufmachung offiziellen E-Mails bekannter Unternehmen täuschend ähnlich ist. Auf diese Weise soll das Vertrauen der Kunden erschlichen werden. Über Links in solchen E-Mails werden die Kunden auf Webseiten geführt, die jenen der betreffenden Unternehmen täuschend echt nachempfunden sind. Durch entsprechende Aufforderungen versuchen die Betrüger hier nun, Nutzerdaten auszuspähen und an Passwörter, Daten für das Online-Banking oder Kreditkartennummern zu gelangen. Diese Informationen werden dann für Finanztransaktionen missbraucht.

Waren die gefälschten E-Mails und Webseiten in den Anfangszeiten des Phishing noch primitiv aufgemacht, wurde deren Gestaltung mittlerweile deutlich professionalisiert und individualisiert. Das führte dazu, dass Kunden heute kaum mehr zwischen authentischen und gefälschten E-Mails unterscheiden können. Diverse Aufklärungsmaßnahmen durch Banken, Behörden und Medien haben allerdings dazu geführt, dass Kunden immer vorsichtiger im Umgang mit Phishing-Mails werden und den Passwortfischern seltener in die Netze gehen.

Außerdem werden die Domains, unter denen die Phisher aktiv werden, immer schneller erkannt und gesperrt, wodurch die „Lebensdauer“ der betrügerischen Link-Adressen drastisch zurückgeht. Die Kriminellen haben darauf allerdings bereits reagiert und setzen verstärkt Trojanische Pferde ein, um an vertrauliche Kundendaten zu gelangen. Nach Aussage der Banken sind die in Deutschland im Jahr 2006 eingetretenen Schadensfälle nur noch zu rund zehn Prozent auf die klassische E-Mail-Methode zurückzuführen. Für die restlichen 90 Prozent zeichnen Trojanische Pferde verantwortlich.

Art der Phishing-Vorfälle



Quelle: BSI

Abbildung 9: Aufteilung der Phishing-Vorfälle nach Art des Angriffs im Jahr 2006 [3]

Zur Erhöhung des Sicherheitsniveaus in Deutschland haben sicher auch neue Modelle wie iTAN, mTAN oder smsTAN beigetragen, die das bestehende PIN-TAN-Verfahren um weitere Sicherheitsstufen ergänzen. Auch das Home Banking Computer Interface (HBCI) mit seiner Anforderung an eine Chipkarte und einen Chipkartenleser bietet eine alternative Absicherung.

Neben den Geldinstituten geraten zunehmend auch E-Commerce-Anwendungen und Online-Shops ins Visier der Phisher. Ziele sind dabei auch mittelständische Unternehmen, die über keine IT-Sicherheitsabteilung verfügen. Abgefischt werden häufig nicht nur kurzfristige Zugangs- und Transaktionsdaten, sondern auch Informationen zur Identität wie etwa Geburtsdatum, Anschrift und Führerscheinnummern sowie Konten- und Kreditkartennummern. Mit diesen Daten werden dann kriminelle Aktivitäten durchgeführt. Für die Opfer bedeutet es oft große Mühe, ihre Unschuld zu beweisen. Wesentliche Maßnahmen der Bundesregierung zur Gewährleistung einer gesicherten elektronischen Identität und zum Schutz vor Identitätsdiebstahl sind die Einführung des elektronischen Personalausweises und die Förderung von Bürgerportalen im Rahmen des Programms E-Government 2.0. Durch beide Projekte wird eine verbindliche Authentisierung von Bürgerinnen und Bürgern und Diensteanbietern in der elektronischen Welt ermöglicht.

4.7 Dialer und Ping-Anrufe

Dialer sind Computerprogramme, mit denen sich eine Verbindung zum Internet aufbauen lässt. Mehrwertdienste im Internet, wie zum Beispiel kostenpflichtige Informationen oder Downloads, werden so über die Telefonrechnung (Micro-Payment) belastet. Dazu muss der Betreiber eines Dialers eine Zulassung bei der Bundesnetzagentur (BNetzA) beantragen.

Der Einsatz von illegalen Dialern, die sich unbemerkt auf Computern installieren und über teure Rufnummern Internetverbindungen herstellen, ist in den letzten Jahren stark zurückgegangen. Gründe dafür sind neue Verfahren der Telekommunikationsanbieter, die solche Programme aufgrund von Verbindungsanalysen bereits frühzeitig entdecken, sowie gesetzliche Regelungen.

Die Betrüger greifen allerdings auf neue Methoden zurück, die so genannten Spam- oder Ping-Anrufe. Das Telefon klingelt kurz, danach wird die Anwahl sofort beendet. Im Telefondisplay erscheint eine Rufnummer in der Liste der entgangenen Gespräche. Diese Telefonnummer soll den Angerufenen zu einem teuren Rückruf veranlassen.

Opfer derartiger Betrügereien können die betreffenden Nummern der Bundesnetzagentur melden. Sie bearbeitet schriftliche und telefonische Verbraucheranfragen und Beschwerden und ergreift Maßnahmen zur Bekämpfung, wenn gesicherte Kenntnisse zu Missbrauchsfällen vorliegen.

4.8 Innentäter, Irrtum und Nachlässigkeit

Nicht nur schadhafte Programme und kriminelle Angreifer stellen Sicherheitsrisiken für die IT-Systeme eines Unternehmens dar. Studien weisen immer wieder eine akute Bedrohung durch Irrtum und Nachlässigkeit der Anwender selbst nach. Besonders gravierend sind Vorfälle im Arbeitsumfeld. Der Anwender schadet dabei nicht nur sich selbst, sondern verursacht mitunter einen beträchtlichen Schaden für das gesamte Unternehmen.

Risiken liegen beispielsweise in einem nachlässigen Umgang mit vertraulichen Daten oder in der Weitergabe von Authentisierungsmedien, wie zum Beispiel Token oder Chip-Karten. Aber auch der Anschluss privater Hardware an

Firmen-PCs birgt große Gefahren für Firmennetzwerke, die auf diesem Weg mit Computerschädlingen infiziert werden können. So schließen mehr als die Hälfte der Befragten einer Studie eigene Peripherie-Geräte wie zum Beispiel USB-Sticks und Fotokameras an den Firmen-PC an. Knapp ein Fünftel der Befragten überlässt Freunden und Familienangehörigen das Notebook, um zu surfen oder zu spielen.[12] Darüber hinaus stellen natürlich auch jene Mitarbeiter eine Gefahr für das Unternehmen dar, die der Firma aus Rache, Neid oder aus Motiven der persönlichen Bereicherung vorsätzlich Schaden zufügen.

Vielen Arbeitnehmern ist für nachlässiges Verhalten aber nur bedingt ein Vorwurf zu machen. Problematisch ist vor allem, dass Unternehmen zu selten die notwendigen Vorsichtsmaßnahmen ergreifen, um die Gefahr abzuwenden, die von den so genannten Innentätern ausgeht.

IT-Sicherheit in innovativen Technologien

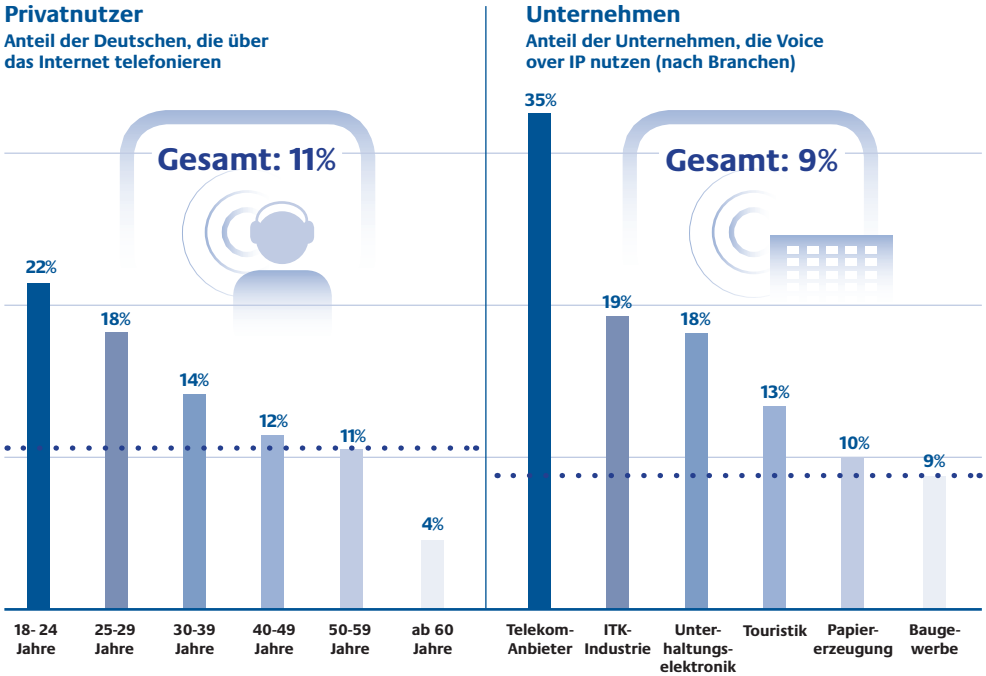
5 IT-Sicherheit in innovativen Technologien

Innovative Technologien sichern Zukunftsfähigkeit. Durch Technologietransfer eröffnen sich Chancen für Wirtschaft und Gesellschaft. Die Komplexität der neuen Entwicklungen bringt aber auch Risiken für Hersteller und Anwender mit sich.

5.1 Voice over IP - VoIP

Sprach- und Datendienste werden immer enger miteinander verknüpft. Ein Beispiel dafür stellt die Internettelefonie bzw. Voice over Internet Protocol (VoIP) dar. Elf Prozent der Deutschen nutzen bereits privat VoIP. Bei den Unternehmen sind es erst neun Prozent.[13] Eine Umfrage unter IT-Managern und Sicherheitsverantwortlichen ergab allerdings, dass rund 30 Prozent der befragten Unternehmen den Einsatz planen.[5]

Voice over IP: Privatnutzer vor Unternehmen



Quelle: BITKOM

Abbildung 10: Verbreitung der Internet-Telefonie in Deutschland [13]

VoIP-Technologien können aus dem Blickwinkel der IT-Sicherheit eine Bedrohung darstellen. Im Vergleich zu herkömmlichen Telekommunikationsanlagen ist ihr ungesicherter Einsatz mit deutlich größeren Risiken verbunden. Denn zu den Sicherheitsrisiken der TK-Welt, beispielsweise der Manipulation durch aktivierte Fernwartungsmechanismen, kommen die der IP-Welt unter anderem DoS-Angriffe oder der Befall durch Schadprogramme hinzu. Mit der Verbreitung steigt auch die Anzahl der Angriffe auf VoIP-Systeme.

Die Zusammenlegung von IP-Kommunikation und Telekommunikation führt auch dazu, dass beide Dienste gleichzeitig gestört werden oder ausfallen können. Für einen verlässlichen Betrieb von VoIP-Systemen müssen daher Sicherheitsmaßnahmen in beiden Technologien frühzeitig in die Planungen einbezogen werden. Dazu zählt unter anderem die Entwicklung passender Firewall- und Notrufkonzepte und QoS (Quality of Service)-Maßnahmen in IP-basierten Sprachnetzen.

5.2 Mobile Kommunikation – WLAN, Handy, Bluetooth

Multimedia Messaging Services (MMS), E-Mail und Internetverbindungen, Wireless LAN (WLAN), Bluetooth-Schnittstellen, Werkzeuge zur Synchronisation mit PCs, austauschbare Speicherkarten – all diese Formen mobiler Kommunikation stellen Einfallschleusen für die Infektion mit Schadprogrammen dar. Die meisten dieser Funktionen sind in heutigen Mobilgeräten standardmäßig integriert. Das macht es Anwendern zwar besonders einfach, diese Technologien zu nutzen, steigert gleichzeitig aber das Gefährdungspotenzial. Schutzmaßnahmen wie Virenscanner oder Firewalls werden zwar mittlerweile auch für eine Reihe mobiler Endgeräte angeboten, sind jedoch kaum verbreitet. Mobile Sprach- und Datenkommunikation wird derzeit vornehmlich über GSM- und UMTS-Mobilfunknetze und im lokalen Bereich zunehmend über WLAN durchgeführt.

Mobile Datenübertragung – WLAN

WLAN-Verbindungen werden zumeist zur Erweiterung kabelgebundener LANs sowie zum Zugriff auf das Internet in öffentlichen Bereichen (Hotspots) bzw. als Bestandteil von DSL-Routern eingesetzt. Im privaten Bereich liegt die Nutzungsrate laut einer BSI-Studie bereits bei 27 Prozent. Auch im Unterneh-

mensbereich werden mobile Funknetzwerke in Deutschland immer häufiger eingesetzt, wobei gilt: Je größer das Unternehmen, desto eher werden WLANs betrieben.[5] Bei Laptops gehören integrierte WLAN-Module mittlerweile zur Standardausstattung.

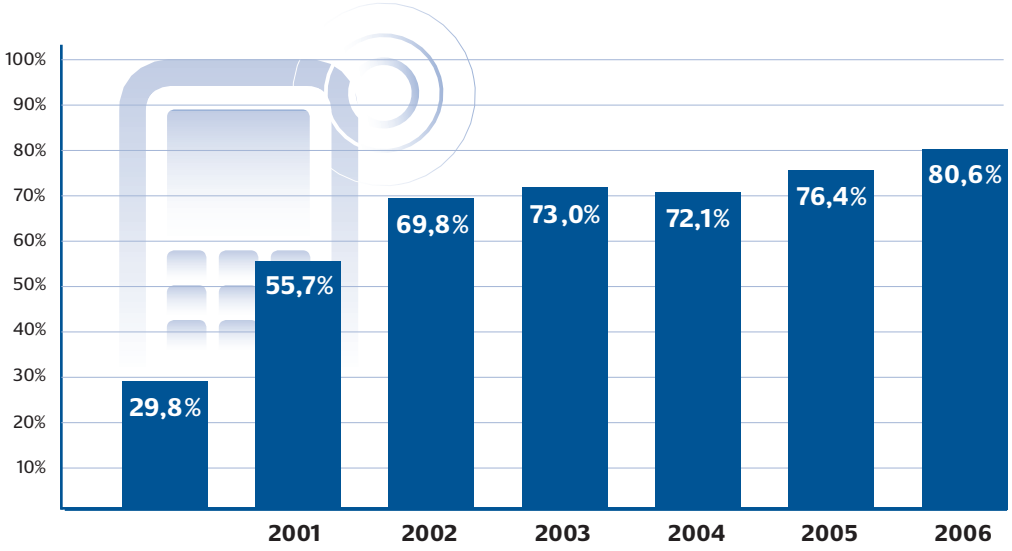
Ist ein WLAN aber nicht ausreichend gesichert, können Angreifer nicht nur in Unternehmensnetzwerke eindringen und vertrauliche Daten sammeln, sondern beispielsweise auch Spam-Mails versenden. Dadurch können Unternehmen massiv geschädigt werden – nicht nur finanziell, sondern auch durch Imageschäden.

Insgesamt geht der Anteil offener WLANs tendenziell zurück – auch wenn es hier Abweichungen in den Erhebungen je nach Region und Quelle gibt. In der Summe ist die Sicherheitslage aber weiterhin bedrohlich, da zumeist schwache Sicherheitsmechanismen (WEP) eingesetzt werden. Die verbesserten Mechanismen des Sicherheitsstandards IEEE802.11i (auch bekannt als WPA2) kommen nur selten zum Einsatz, obwohl diese mittlerweile häufig in die Produkte integriert sind. Hier sind verstärkte Anstrengungen der Hersteller notwendig, damit WLANs mit voreingestellten Sicherheitsmerkmalen ohne wesentliche Benutzeraktivitäten sicher in Betrieb gehen. Das BSI hat mit der Technischen Richtlinie zum sicheren Einsatz von WLAN Sicherheitsfunktionalitäten von WLAN-Produkten für Hersteller und Prüfinstanzen definiert und Verfahren zur Prüfung angegeben.

Mobile Kommunikation – Handy, PDA, Bluetooth

In 80,6 Prozent der deutschen Haushalte besaß im Jahr 2006 zumindest eine Person ein Mobiltelefon – im Jahr zuvor waren es 76,4 Prozent.[14]

Verbreitung von Mobiltelefonen



Quelle: Statistisches Bundesamt

Abbildung 11: Ausstattung von Haushalten mit Mobiltelefonen 2000 bis 2006 in Prozent [14]

Moderne Mobiltelefone werden dabei immer mehr zu smarten Computern mit eigenem Betriebssystem sowie einer Vielzahl von Funktionen, Anwendungen und Schnittstellen. Sie sind damit einer Reihe von Risiken ausgesetzt – von Verlust bzw. Diebstahl bis hin zur Infektion mit Schadprogrammen. Derzeit ist das Risiko einer Infektion mobiler Endgeräte im Vergleich zu PCs zwar noch gering, aber durchaus realistisch. Die Anzahl bekannter Schadprogramme für mobile Endgeräte ist seit ihrem ersten Auftreten 2004 auf einen dreistelligen Wert angestiegen, Tendenz weiter steigend. Allerdings haben nur rund eine Handvoll Schadprogramme weltweite Bedeutung erlangt.

Im Zusammenhang mit Sicherheitsfragen ist insbesondere die Bluetooth-Schnittstelle an mobilen Endgeräten in Kritik geraten. Der symmetrische Schlüssel für die Authentisierung und Verschlüsselung wird hier direkt von der vom Nutzer eingegebenen PIN abgeleitet. Typische Gewohnheiten bei der Wahl

der PINs können daher für Angriffe ausgenutzt werden. Auf Herstellerseite ist zudem die nachlässige Implementierung der Schnittstellen für die Bluetooth-Programmierung (Bluetooth-Stacks) zu bemängeln. Angreifer können diese Schwächen ausnutzen, um vertrauliche Informationen auszulesen oder Geräte gar für ihre Zwecke zu missbrauchen.

5.3 Asynchrones JavaScript und XML (AJAX)

Verbunden mit dem Schlagwort Web 2.0 entstehen aktuell vielerorts innovative Webanwendungen. Eine davon ist AJAX, die asynchrone Verbindung von JavaScript und XML. Die Besonderheit bei AJAX-Anwendungen besteht darin, dass Inhalte weitgehend unbeeinflusst vom Nutzer in eine bestehende Webseite nachgeladen werden können. Abgeänderte Webseiten müssen so nicht komplett neu übertragen und aufgebaut werden, der Anwender muss nicht auf das Nachladen warten. Es wird damit möglich, Desktop-ähnliche Anwendungen über das Web anzubieten.

Aus Sicht des BSI ist das dafür notwendige Freischalten der Browser für die Ausführung Aktiver Inhalte wie JavaScript kritisch zu bewerten. Diese Bedenken verschärfen sich in jüngster Zeit, denn bösartige Aktive Inhalte werden immer öfter dazu genutzt, gezielt Trojanische Pferde in vertrauenswürdige Umgebungen von Unternehmen und Behörden einzuschleusen und dort unbemerkt Datenspionage zu betreiben.

Sicher eingesetzt werden können Techniken wie AJAX-Webanwendungen in schutzbedürftigen Umgebungen nur über speziell abgesicherte Terminal-Server-Lösungen, wie beispielsweise dem vom BSI entwickelten ReCoBS (Remote Controlled Browsers System).

5.4 Prozesssteuerungssysteme – SCADA

Die ständige Verfügbarkeit von Infrastrukturen etwa zur Strom- oder Wasserversorgung spielt für Unternehmen, Verwaltungen und private Haushalte eine große Rolle. Dort kommen spezielle Prozesssteuerungssysteme und SCADA (Supervisory Control and Data Acquisition)-Systeme zur Steuerung der verschiedenen Funktionen zum Einsatz. Auch aus der Verarbeitungs- und Produktions-

industrie sind solche Systeme nicht mehr wegzudenken. Zur Vernetzung ihrer Komponenten nutzen diese Systeme oftmals die gleiche Technologie wie Computernetzwerke. Hat ein Angreifer von außen Zugriff auf das Netzwerk eines Prozesssteuerungssystems, kann er die gleichen Angriffsmethoden nutzen, die gegen Standard-Informationstechnik eingesetzt werden.

Bei vielen SCADA-Systemen können herkömmliche Schutzmaßnahmen aufgrund der besonderen Anforderungen nicht ohne Weiteres angewandt werden. Deshalb ist das Gefahrenpotenzial groß. Netzwerkmonitore, Intrusion-Detection-Systeme und der Einsatz von Firewalls mit sehr restriktiven Regeln können zwar einen wichtigen Beitrag leisten, ihr Einsatz kann die Funktionsfähigkeit der Prozesssteuerungssysteme aber beeinträchtigen.

Die Wechselwirkungen zwischen IT-Sicherheit und der Sicherheit von Prozesssteuerungssystemen werden seit einigen Jahren intensiv diskutiert. Immer mehr Hersteller, Integratoren und auch Betreiber von Prozesssteuerungssystemen erkennen die Notwendigkeit geeigneter IT-spezifischer Sicherheitsmaßnahmen. Bei der Entwicklung vieler existierender und bereits im Einsatz befindlicher SCADA-Komponenten ist der Aspekt der IT-Sicherheit allerdings noch nicht ausreichend berücksichtigt worden. Sicherheitsmechanismen wie Authentifizierung und Verschlüsselung wurden in der Prozesssteuerungstechnik selbst nur unvollständig oder gar nicht implementiert. Insbesondere bei der Erstellung und Fortschreibung von Sicherheitskonzepten für ältere Prozesssteuerungssysteme wird die Gefahr weiterhin unterschätzt.

5.5 Radio Frequency Identification – RFID

RFID bezeichnet Verfahren zur automatischen Identifizierung von Objekten über Funk. RFID-Systeme kommen dort zum Einsatz, wo automatisch gekennzeichnet, erkannt, registriert, gelagert, überwacht oder transportiert werden muss, etwa bei der elektronischen Kfz-Diebstahlsicherung oder der Kombination von Unternehmensausweisen mit Zutrittskontrollanlagen.

Werden dabei personenbezogene Daten mit RFID-Unterstützung verarbeitet, sind die Grundsätze des Datenschutzrechts zu berücksichtigen. Die fortschreitende Entwicklung in der Mikroelektronik wird in der Zukunft auch RFID-Tags ermöglichen, die auf sensorische Reize, Bewegungen und Verformungen

reagieren. Damit werden neue Anwendungen möglich, etwa zur Kontrolle lückenloser Kühlketten.

Durch neue Einsatzmöglichkeiten und den wachsenden Funktionsumfang von RFID-Systemen nehmen aber auch die Angriffsmöglichkeiten zu. Die grundsätzlichen Gefährdungspotenziale von RFID-Systemen sind das unautorisierte Auslesen oder Verändern von Daten, das Fälschen von Transpondern und das Stören der Kommunikation zwischen Transponder und Lesegerät. Durch DoS-Angriffe kann die Verfügbarkeit von Funktionen eines RFID-Systems beeinträchtigt werden. Sicherheitsmechanismen wie Authentisierung, Verschlüsselung und Abschirmung müssen daher integriert werden.

5.6 Biometrie und Personaldokumente

Seit November 2005 werden in Deutschland elektronische Reisepässe ausgegeben. Deutschland ist damit eines der ersten EU-Länder, das die Vorgaben der entsprechenden EG-Verordnung umsetzt. Im ePass sind so genannte biometrische Daten in einem Radio-Frequency-Chip (RF-Chip) gespeichert. Zunächst werden digitale Passfotos erfasst, ab November 2007 in elektronischen Pässen der zweiten Generation zusätzlich auch Fingerabdrücke. Mit dem ePass wird ein Höchstmaß an Fälschungssicherheit erreicht. Auch die Sicherheit vor dem Missbrauch echter Pässe durch unberechtigte Personen wird erhöht, denn der Chip erlaubt eine elektronische Überprüfung, ob der Nutzer des Dokuments tatsächlich der Passinhaber ist.

Bei der Ausarbeitung der technischen Standards in den europäischen Gremien waren Datenschutz und Datensicherheit ein wichtiges Anliegen. Das BSI war federführend an der Entwicklung von Schutzmechanismen gegen unberechtigte Zugriffe auf die im Chip gespeicherten Daten beteiligt.

Mit Blick auf die internationale Interoperabilität der neuen Pässe und Lesegeräte ist die Entwicklung von Konformitätsstandards von besonderer Bedeutung. Auch hier engagiert sich das BSI. Das erworbene Know-how kann dabei für weitere Anwendungsbereiche nutzbar gemacht werden. Beispielsweise wurde im Koalitionsvertrag 2005 der Einsatz biometrischer Verfahren auch für Personalausweise, Visa und Aufenthaltstitel vorgesehen. Entsprechende Vorbereitungen auf nationaler und europäischer Ebene sind angelaufen.

5.7 Sicherheit von Produkten

Digital Rights Management / Kopierschutz

Die Digitale Rechteverwaltung (englisch Digital Rights Management, kurz DRM) schützt Urheber oder Verwerter digitaler Daten vor deren unberechtigter Verwendung und Verbreitung durch Dritte. Herausgeber von Audio-CDs oder Video-DVDs versuchen dadurch beispielsweise die unrechtmäßige Vervielfältigung ihrer Produkte zu verhindern. Eine entsprechende CD oder DVD lässt sich so etwa auf einem Windows-PC nur abspielen, wenn zuvor eine auf dem Medium enthaltene Software installiert wird. Die Installation der Software führt zu wesentlichen Modifikationen am Betriebssystem. Das wird allerdings in der Lizenzvereinbarung oft verschwiegen bzw. von den meisten Anwendern nicht erkannt.

Manche Kopierschutz-Software installiert spezielle Filter-Treiber, welche die Zugriffe auf CD/DVD-Laufwerke prüfen. In einigen Fällen verhindern diese Filter jedoch nicht nur das Kopieren der zu schützenden Medien, sondern beeinträchtigen auch die reguläre Nutzung von Laufwerken. Darüber hinaus haben Sicherheitsexperten bei der Analyse einiger Kopierschutzprogramme festgestellt, dass die schlechte Programmierung der Software zu Systemabstürzen oder Performanceverlusten führen kann, selbst wenn kein Medium im CD/DVD-Laufwerk eingelegt ist.

Teilweise versteckt sich die Kopierschutz-Software im System, um eine Umgehung des Schutzes durch den Anwender zu verhindern. Damit bilden die Hersteller „Rootkit“-Funktionalitäten nach, die auch Angreifer nutzen, um ihre Aktivitäten zu verschleiern. Manche dieser Funktionen sind so programmiert, dass sie alle Dateien, Registrierungseinträge und Prozesse unsichtbar machen, die mit einem bestimmten Präfix im Namen beginnen. Dies kann von Angreifern ausgenutzt werden, um weitere Programme vor dem Anwender zu verstecken. Diese Schwachstelle wurde bereits von Schadprogrammen ausgenutzt.

Desktop Firewalls / Personal Firewalls

Als Desktop Firewall (auch Personal Firewall) bezeichnet man eine Software, die den Datenverkehr eines an ein Netz angeschlossenen Computers filtert und ihn damit vor Angriffen von innen und außen schützen soll. Die immer häufigere Verwendung von Spionage-Programmen gegen Unternehmen und Behörden machen Desktop Firewalls zu einer unverzichtbaren Schutzmaßnahme.

Die meisten Desktop Firewalls schützen bei korrekter Konfiguration sehr gut vor externen Angriffen auf den Rechner. Das Herausschleusen von Daten durch Firewall-Bypass-Techniken und so genannte Covert Channels (verdeckte Kanäle) lässt sich allerdings nicht vollständig verhindern.

Zu den häufigsten Risikofaktoren beim Einsatz von Desktop Firewalls zählt – neben der bewussten Deaktivierung durch den Benutzer – die fehlerhafte Installation. Die Folge ist eine trügerische Sicherheit, die mitunter schwerwiegende Folgen haben kann. Ist die Desktop Firewall stärker als beabsichtigt für unerwünschte Verbindungen geöffnet und somit ihre Schutzwirkung negativ beeinträchtigt, ist der Privatnutzer Gefahren weitgehend schutzlos ausgeliefert.

Auch in Unternehmen und Behörden können Desktop Firewalls eine nützliche Ergänzung zu den sonstigen IT-Sicherheitsmaßnahmen darstellen. Allerdings kommen sie dort bislang kaum zum Einsatz. Die Gründe dafür liegen nicht nur in einer fehlenden Sensibilisierung der Verantwortlichen gegenüber Trojanischen Pferden und Spionageprogrammen, sondern auch im Mehraufwand insbesondere bei der Installation und ersten Konfiguration.

5.8 Trusted Computing

Trusted Computing stellt einen neuen Ansatz dar, die Sicherheit von IT-Systemen zu erhöhen. Ein neuer Hardware-Baustein soll in Zukunft die Sicherheit von Betriebssystem-Plattformen und die gegenseitige Authentisierung von Computern ermöglichen. Dieser Baustein wird von einer Gruppe von Unternehmen, die sich als Trusted Computing Group (TCG) zusammen geschlossen haben, unter dem Namen Trusted Platform Module (TPM) erstellt. Die zum großen Teil frei zugänglichen Spezifikationen werden von der TCG laufend überarbeitet und aktualisiert. Bereits jetzt dienen sie als Grundlage für die millionenfache Produktion von TPM-Chips, die in Computer, Mobiltelefone und sonstige IT-Produkte integriert werden.

Die breite Einführung des TPM wird erhebliche Auswirkungen auf den Umgang mit Sicherheit in der Informationstechnik haben. Viele Rechner werden bereits mit TPM angeboten, ohne jedoch die damit verbundenen Sicherheitsfunktionen vollständig zu nutzen. Eine breitere Anwendung ist mit dem neuen Microsoft Betriebssystem VISTA zu erwarten.

5.9 Grid-Computing

Grid (Gitternetz)-Computing verbindet Hardware-, Software- und Daten-Ressourcen von verteilten Supercomputing-Zentren und nutzt sie für besondere, etwa sehr ressourcenintensive Anwendungen. Rechenleistung aus diesem Gitternetz könnte demnach so einfach abrufbar sein wie der elektrische Strom aus dem Stromnetz (englisch Power Grid). Bereits heute gibt es eine vielfältige Zahl praktischer Anwendungsmöglichkeiten von der Wissenschaft bis hin zum konkreten Einsatz in der Medizin.

Die Überwindung der Domänengrenzen zwischen technisch und rechtlich autonomen Organisationen bringt allerdings auch Probleme mit sich. Neben den technischen Herausforderungen der geeigneten Parallelisierung, der Verfügbarkeit und der Zuverlässigkeit ergeben sich auch neue Herausforderungen an die Sicherheit. Dabei ist zwischen unternehmensinternen und unternehmensübergreifenden Grids zu unterscheiden.

Bei einer unternehmensinternen Verarbeitung sensibler Daten ergeben sich insbesondere Risiken bezüglich der Vertraulichkeit und der Integrität dieser Daten. Diese lassen sich in der Regel durch organisatorische Maßnahmen reduzieren. Beim Einsatz eines unternehmensübergreifenden Grids empfehlen sich konkrete vertragliche Vereinbarungen, beispielsweise im Rahmen eines Service Level Agreements, in dem anwendungsspezifische Sicherheitsanforderungen und deren Umsetzung vorab vereinbart und überprüft werden.

Trends

6 Trends

Im Lagebericht 2005 wurden Trends vorgestellt, die in 2007 größtenteils alltägliche Realität sind. So setzt sich der Trend in Richtung einer Professionalisierung und einer Fokussierung auf wirtschaftlichen Gewinn bei den Programmierern von Schadprogrammen bis heute fort. Der Wirtschaftsspionage wird weiterhin ein starker Anstieg prognostiziert.[6] Auch die Regionalisierung von Schadprogrammen, das heißt vermehrt deutschsprachige Texte und sogar persönliche Ansprachen in E-Mails mit schadhaften Anhängen, ist weiter vorangeschritten und mittlerweile die Regel.

IT-Sicherheit ist keine isolierte Materie. Aktuelle Veränderungen in Wirtschaft und Gesellschaft spiegeln sich in ihr ebenso wider wie technologischer Fortschritt und rechtliche Trends. Die Kenntnis solcher Entwicklungen kann viel dazu beitragen, die Bedeutung von IT-Sicherheit besser einschätzen und verstehen zu können. Die folgenden Abschnitte geben einen Überblick über verschiedene Trends, die die Bedeutung von IT-Sicherheit künftig beeinflussen werden.

6.1 Wirtschaftliche und gesellschaftliche Trends

Wissen und Innovation als zentrale Wirtschaftsgüter

Der Übergang von der industriellen Gesellschaft hin zur Wissensgesellschaft führt zu einer immer intensiveren weltweiten Vernetzung der Informationsströme. Wissen und Innovation stellen dabei die zentralen Objekte der Wertschöpfung dar. Dem Schutz dieser Ströme, die zunehmend zum Ziel von Angriffen auch in Form organisierter Kriminalität werden, kommt daher steigende Bedeutung zu. Eine Studie kam zu dem Schluss, dass 40 Prozent aller Organisationen bis zum Jahr 2008 Ziel finanziell motivierter krimineller Angriffe werden.[15]

Das Sicherstellen der Kontinuität von Geschäftsprozessen (Business Continuity) im Krisenfall und die Entwicklung präventiver Maßnahmen zeigt sich deshalb als wesentliche Managementaufgabe – schließlich können durch Betriebsausfälle gewaltige Kosten entstehen, der Verlust von Kundendaten oder internen Informationen über Geschäftsabläufe kann massive Wettbewerbsnachteile

mit sich bringen. Eine 2006 weltweit durchgeführte Studie zeigt bei der Implementierung von Maßnahmen allerdings große Branchenunterschiede: Während im Finanzdienstleistungssektor 88 Prozent über unternehmensweite Business Continuity-Programme und einen Chief Information Security Officer verfügten, lag die Zahl im Bereich der Technologie-, Medien- und Telekommunikationsunternehmen nur bei rund 50 Prozent.[16]

Verlagerung von Verwaltungs- und Geschäftsaktivitäten ins Internet

Einkaufen im Internet wird in Deutschland immer populärer. Der Umsatz des elektronischen Handels wird nach Schätzungen von Marktforschungsunternehmen bis zum Jahr 2009 auf rund 694 Milliarden Euro ansteigen – im Jahr 2005 waren es noch 321 Milliarden Euro.[17] 78 Prozent der Teilnehmer einer Umfrage unter deutschen Unternehmen begreifen eBusiness und die damit verbundene Optimierung von Geschäftsprozessen bereits als Teil ihres Tagesgeschäfts. Auch die Bereitschaft zu Investitionen in den elektronischen Handel steigt vor allem bei kleineren deutschen Unternehmen im Vergleich zu den Vorjahren deutlich an.[18] Die Nachfrage ist gegeben: Zum Ende des Jahres 2006 erledigten bereits 31,4 Millionen Deutsche Einkäufe über das Internet.[17] Die verstärkten E-Commerce-Aktivitäten lassen auch neue Geschäftsmodelle entstehen. Dass dort hohe Umsätze zu erwarten sind, zeigt beispielsweise der Einstieg wirtschaftlich erfolgreicher IT-Unternehmen in den Online-Handel mit Musik- und Videodateien.

Auch die Verwaltung setzt zunehmend auf Internetservices. Im September 2006 waren insgesamt mehr als 440 Dienstleistungen der Bundesbehörden online verfügbar. Die Bundesländer setzen eigene E-Government-Strategien um, nahezu alle Kommunen verfügen über eine Internetpräsenz. In den Monaten September bis November 2006 nutzten 49 Prozent der Unternehmen das Internet für Interaktionen mit Behörden, 28 Prozent der Bundesbürger haben in diesen drei Monaten das Internet zur Informationsbeschaffung auf Webseiten öffentlicher Stellen genutzt.[19]

In den nächsten Jahren sollen die bereits bestehenden elektronischen Dienstleistungen vertieft und insbesondere die Orientierung am Bedarf der Nutzer noch verstärkt werden. Formelle Basis dafür bietet das 2006 beschlossene Programm E-Government 2.0, das auch die Belange der IT-Sicherheit einbezieht. So wird zum Beispiel im Handlungsfeld „Prozessketten“ angestrebt, für alle zu realisierenden Prozessketten eine IT-Grundschutz-Zertifizierung durchzuführen.

Auch auf internationaler Ebene wurde mit der EU-Initiative i2010 ein Rahmen für den Ausbau von E-Government geschaffen. Darin verpflichten sich die Mitgliedsstaaten unter anderem dazu, bis 2010 sichere Systeme für die gegenseitige Anerkennung nationaler elektronischer Identitäten für Internetangebote und Dienste der öffentlichen Verwaltungen zu schaffen.

Der Anstieg der geschäftlichen und verwaltungstechnischen Internetaktivitäten könnte in manchen Bereichen allerdings auch zu neuen Herausforderungen für die IT-Sicherheit führen: Zum einen bieten sich alleine durch die höhere Online-Frequenz mehr Möglichkeiten zu Infektionen mit Schadprogrammen. Darüber hinaus werden im Zuge dieser Aktivitäten verstärkt sensible Informationen über das Internet ausgetauscht, wodurch sich neue Möglichkeiten für Online-Kriminalität bieten. So wie Wirtschaft und Verwaltung neue Modelle entwickeln, passen auch Kriminelle ihre Aktivitäten den neuen Gegebenheiten an und überraschen Organisationen wie Nutzer mit neuen Angriffsformen.

Web 2.0 - Steigende Ansprüche an Interaktivität und Mobilität

Als Web 2.0 wird der – in diesem Bericht bereits an unterschiedlichen Stellen angesprochene – massive Anstieg der Interaktivität in der virtuellen Welt bezeichnet. Das Internet bietet immer neue Techniken und Dienste, die den direkten Austausch von Informationen ermöglichen. Die Nutzer werden dadurch zu einem immer freizügigeren Umgang mit persönlichen Daten angeregt, etwa in Blogs, auf offenen Webseiten oder in Diskussionsforen. Die Kommunikation richtet sich dabei in der Regel nicht an klar definierte Zielpersonen, die darin enthaltenen Informationen können daher auch von böswilligen Dritten missbraucht werden. Kriminelle, wie etwa Datenfischer, haben sich auf diese Entwicklung bereits eingestellt: Sie gehen verstärkt individualisiert, mit persönlicher Anmutung auf ihre Opfer zu und bauen so ein Vertrauensverhältnis auf (Social Engineering), das sie dann zum Ausspionieren privater Daten, etwa Zugangskennwörter für das Online-Banking, missbrauchen. Ein weiterer sicherheitsrelevanter Aspekt der Interaktivität: In Blogs oder Foren ist kaum mehr erkennbar, ob Inhalte nur private Meinungen widerspiegeln oder werbliche Zwecke verfolgen – auch in Sicherheitsfragen wird dadurch eine seriöse Meinungsbildung zunehmend erschwert.

Was die technischen Voraussetzungen betrifft, so bezeichnet eine aktuelle Studie das Jahr 2006 als Jahr der Konsolidierung: PCs wurden in der Mehrzahl

der Fälle fit für die Anforderungen von Web 2.0 gemacht und auch Zusatzelemente wie Webcams und Headsets gehören immer häufiger zur Ausstattung.[20]

PC-Ausstattung 2004 bis 2006 in Prozent

Ausstattung	2004	2005	2006
DVD-Laufwerk	72	79	82
CD-Brenner	72	77	73
DVD-Brenner	37	56	57
Kopfhörer/Mikrofon (Headset)	–	–	39
USB-TV-Karte	–	–	25
TV-Karte	24	28	21
Webcam	–	–	17

Quelle: ARD/ZDF

Abbildung 12: PC-Ausstattung von Online-Nutzern über 14 Jahre in Deutschland [20]

Demografischer Wandel und spezielle Bildungsangebote

In unserer Gesellschaft steigt die Zahl älterer und alter Menschen, die verstärkt die Möglichkeiten der Kommunikationstechnik nutzen. Mittlerweile nutzen bereits 33,7 Prozent der Menschen ab 50 das Internet.[21] Für diese auch als Silver Surfer bezeichnete Gruppe existieren zahlreiche IT-Bildungsangebote, die spezifisch auf ihre Bedürfnisse eingehen und in denen vielfach auch die IT-Sicherheit zur Sprache kommt. Die Silver Surfer messen der Information über Sicherheit im Vergleich zu anderen Altersgruppen eine höhere Bedeutung zu: So wollen etwa mehr als zwei Drittel regelmäßig E-Mail-Informationen zu aktuellen Sicherheitsproblemen beziehen, in der Gruppe der 14- bis 29-Jährigen äußern nur rund 40 Prozent Interesse an derartigen Angeboten.[21] Die Verschiebung der Alterspyramide könnte also durchaus zu einem höheren Sicherheitsbewusstsein der Computernutzer beitragen. Bildungsmaßnahmen im Bereich der IT-Sicherheit gewinnen jedoch nicht nur im Hinblick auf ältere Bürger an Bedeutung. Auch in der Personalentwicklung von Wirtschafts- und

Verwaltungsorganisationen spielen sie eine immer größere Rolle. Die Integration von IT-Sicherheit in Lehrpläne an Schulen wird ebenso verstärkt gefordert, entsprechende Modelle wurden bereits entwickelt. Während die Zahl der Kampagnen für Bürger zur Steigerung der IT-Sicherheitskompetenz steigt, nimmt die Zahl der präventiven, aufklärenden Medienberichte nur sehr langsam zu – zumeist steht die reaktive Berichterstattung über IT-Krisen noch im Vordergrund.

6.2 Technik-Trends

Unified Threat Management Appliances (UTMA)

In den nächsten Jahren wird in den Unternehmen ein verstärkter Einsatz von so genannten Unified Threat Management Appliances (UTMA) erwartet. Dabei handelt es sich um vorkonfigurierte Geräte, die Sicherheitslösungen wie Firewalls, Intrusion Detection/Prevention-Systeme oder Virtual Private Networks (VPN) sowie Antivirenlösungen auf einer Hardwareplattform vereinen. Als Vorteile – vor allem für kleine und mittelständische Unternehmen – werden von den Herstellern eine einfachere Installation, niedrigere Kosten und eine geringere Komplexität beim Gerätemanagement angeführt. Es kann davon ausgegangen werden, dass in der nächsten Zeit weitere neue und innovative Funktionen in UTMA integriert werden.

Quantencomputer gegen Kryptoverfahren, Quantenkryptographie

Quantencomputer – hocheffiziente, auf einer neuen Technik basierende Rechner – befinden sich derzeit noch in der Phase der Grundlagenforschung. Sollte es gelingen, Quantencomputer in entsprechender Größenordnung zu realisieren, sind viele derzeit weit verbreitete kryptographische Algorithmen de facto gebrochen. Daher befasst sich die Forschung im Hinblick auf Daten, deren Vertraulichkeit, Integrität und Authentizität über einen sehr großen Zeitraum gewährleistet werden soll, bereits heute mit dieser Thematik. Es wird nach Wegen gesucht, wie den potenziellen Sicherheitsgefahren durch Quantencomputer begegnet werden kann. Einerseits werden klassische Algorithmen entwickelt, die resistent gegen Angriffe mit Quantencomputern (quantencomputerresistente Kryptoverfahren) sind, andererseits werden Eigenschaften der Quantenmechanik selbst als Basis für Sicherheitslösungen genutzt (Quantenkryptographie).

Hash-Funktionen

Kryptografische Hashwerte spielen unter anderem bei der Erstellung digitaler Signaturen eine zentrale Rolle. Weltweit verbreitet ist der von der US-Behörde National Institute of Standards and Technology (NIST) standardisierte SHA-1-Algorithmus, in dem allerdings von einem chinesischen Forscherteam bereits Schwachstellen entdeckt wurden. NIST will daher einen Wettbewerb ausrufen, um einen neuen Hash-Standard zu ermitteln. Dieser soll spätestens Ende 2012 in Kraft treten. Berücksichtigt man Vorlaufzeiten und die Lebenszyklen von Chipkarten, kann man allerdings davon ausgehen, dass die bisherigen Hash-Funktionen mindestens noch bis 2018 eingesetzt werden. Bei sicherheitskritischen Signaturanwendungen kommen als Zwischenlösung insbesondere Vertreter der SHA-2-Familie in Frage, die eine Erweiterung von SHA-1 darstellen.

Schlüssellängen / Algorithmen

Das deutsche Signaturgesetz schreibt vor, welche Verfahren als qualifizierte elektronische Signaturen anerkannt werden. Rechtlich maßgeblich für die Zulässigkeit von Algorithmen und Parametern (unter anderem Schlüssellängen) für diese Signaturen ist der so genannte Algorithmenkatalog, ein von der Bundesnetzagentur alljährlich veröffentlichtes Dokument. Hierfür spielt die aktuelle Einschätzung der Sicherheitseigenschaften bzw. von Sicherheitsschwachstellen kryptographischer Algorithmen (zum Beispiel der Hashfunktion SHA-1) eine zentrale Rolle. Bei den derzeit verwendeten Signaturkarten spielt das RSA-Verfahren eine zentrale Rolle. Bis Ende 2007 wird im Algorithmenkatalog eine Schlüssellänge von 1024 Bit für RSA als ausreichend betrachtet, ab Anfang 2011 wird eine Mindestschlüssellänge von 1976 Bit gefordert. Zukünftig könnten aus Gründen der Performanz Verfahren eine größere Bedeutung erlangen, die auf elliptischen Kurven basieren, denn dort garantieren auch kürzere Schlüssellängen eine hohe Sicherheit. Zudem werden moderne Kryptogeräte zukünftig nicht mehr auf anwendungsspezifischen integrierten Schaltungen (ASIC oder Custom-Chip) basieren. Vielmehr geht der Trend hin zu rekonfigurierbarer Hardware.

6.3 Rechtliche Trends

IT-Sicherheit stellt heute einen entscheidenden Faktor in der Wertschöpfungskette dar. Bei geringeren unternehmensinternen Sicherheitsstandards steigt naturgemäß das Risiko schwerer Krisen. Und das bringt nicht nur eine geringere

Kreditwürdigkeit mit sich, sondern unter Umständen auch höhere Haftpflichtversicherungsprämien. Wenn es zum Schadensfall kommt, stellt sich die Frage nach der rechtlichen Verantwortung. Dafür kommen Hersteller oder Dienstleister wie zum Beispiel Internet Provider ebenso in Frage wie die IT-Anwender.

Die Verpflichtung, IT-Sicherheitsmaßnahmen zu ergreifen, lässt sich für private Nutzer aus zivilrechtlichen Haftungsregelungen durchaus herleiten. Aufgrund des geringen allgemeinen Wissensniveaus in Fragen der IT-Sicherheit (siehe Kapitel 3.1) beschränkt sie sich allerdings auf die Einhaltung allseits bekannter Schutzmaßnahmen.

Auf kommerzielle Nutzer von IT-Anlagen können zahlreiche bestehende rechtliche Haftungsregeln direkt angewandt werden. Als Reaktion auf verschiedene Firmenzusammenbrüche sowohl in den USA als auch in Deutschland wurde in den vergangenen Jahren zusätzlich damit begonnen, die Anforderungen an das unternehmensinterne Management in eigenen Gesetzen zu verankern (Stichwort Compliance, die Einhaltung der vom Gesetz vorgeschriebenen Richtlinien und Mindestanforderungen). So hat das Gesetz zur Kontrolle und Transparenz im Unternehmensbereich (KonTraG) in das deutsche Gesellschaftsrecht die Verpflichtung der Unternehmensleitung eingeführt, ein Risikomanagement einzurichten. Hierzu gehören auch der Einkauf und die Implementierung entsprechender IT-Produkte. Auch das Datenschutz- und Telekommunikationsrecht enthält Vorschriften für kommerzielle IT-Nutzer im Zusammenhang mit Daten, die in ihren Systemen kursieren. Rechtliche Verantwortlichkeiten im Bereich der IT-Sicherheit lassen sich auch aus den Aufsichtspflichten im Banken-, Versicherungs- und Finanzsektor ableiten.

Neben den autonomen deutschen Vorschriften zum Risikomanagement wird die IT-Sicherheit auch von internationalen Vereinbarungen berührt, etwa den Regeln zur Prüfung von Fremdkapital unter Basel II. Schließlich werden in einer globalisierten Geschäftswelt auch ausländische Vorschriften für deutsche Unternehmen immer wichtiger, wie zum Beispiel die Vorschriften des US-amerikanischen Sarbanes-Oxley-Act (SOX) für die Berichterstattung von Unternehmen, deren Wertpapiere in USA gehandelt werden.

Aktivitäten

7 Aktivitäten

Die derzeitige Lage der IT-Sicherheit in der Bundesrepublik zeigt einen massiven Handlungsbedarf in allen gesellschaftlichen Gruppen auf. Die Sicherheitskompetenz der Nutzer muss auf allen Ebenen entscheidend verbessert werden. Das BSI hat dazu bereits umfassende Maßnahmen zur Aufklärung und Sensibilisierung ergriffen, aber auch konkrete Hilfestellungen geleistet. Bürger, Unternehmen und Verwaltung können damit die IT-Sicherheit in ihrem jeweiligen Umfeld selbst voran treiben. In einzelnen Bereichen ist zudem gemeinschaftliches Handeln der unterschiedlichen Gruppen erforderlich.

7.1 Bürger

Der Förderung des Sicherheitsbewusstseins bei den Bürgern kommt eine Schlüsselrolle zu. Ein entscheidender Faktor liegt hier in der richtigen Motivation. Erst wenn dem Nutzer der Sinn hinter den einzelnen Maßnahmen klar ist, wird er sie konsequent umsetzen und den Sicherheitsempfehlungen Folge leisten.

Seit Januar 2003 wird der Privatnutzer kompakt und in einfacher Sprache über das Portal www.bsi-fuer-buerger.de zu allen Themen rund um die IT-Sicherheit informiert. Dieses Angebot wurde im vergangenen Jahr durch eine neuen Service ergänzt: Über die Plattform www.buerger-cert.de können Bürger und Verantwortliche in kleinen Unternehmen E-Mail-Newsletter abonnieren, in denen schnell, kompetent und kostenfrei über aktuelle Risiken und Gefahren informiert wird und Handlungsempfehlungen aufgezeigt werden. IT-Sicherheit muss für den Privatanwender also weder zeitaufwendig noch kostspielig sein.

Zentrales Element bleibt allerdings die Eigenverantwortung der Bürger. Als Privatpersonen ebenso wie als Arbeitnehmer oder Kollegen müssen sie negative Auswirkungen konkreter Gefahren vermeiden oder zumindest so gering wie möglich halten. Ein Rundum-Sorglos-Paket gibt es im Bereich IT-Sicherheit nicht und wird es wohl auch nie geben – Aufklärung und Sensibilisierung mit dem Ziel, die Kompetenz der Bürger im Umgang mit PC und Internet sowie die Eigenverantwortung zu stärken, sollten deshalb auch in Zukunft eine bedeutende Rolle spielen.

7.2 Wirtschaft

Das geringe Problembewusstsein in deutschen Unternehmen führt dazu, dass im Bereich der IT-Sicherheit nur unzureichend finanzielle und personelle Mittel zur Verfügung stehen. Insbesondere die Unternehmensleitung muss sich ihrer Verantwortung bewusst werden, denn IT-Sicherheit ist Chefsache. Der Sicherheitsprozess muss auf Leitungsebene initiiert, dann aber von allen Beteiligten im Unternehmen mitgetragen und mitgestaltet werden. Der individuelle Schutzbedarf kann mittels einer Risikoanalyse festgestellt werden. Ganzheitliche, schriftlich fixierte Richtlinien und Vereinbarungen, die den sicheren Umgang mit IT im Arbeitsumfeld regeln, sollten durch Maßnahmen zur Sensibilisierung der Mitarbeiter ergänzt werden. Für die Umsetzung der IT-Sicherheitsstrategie müssen die erforderlichen personellen und finanziellen Ressourcen zur Verfügung gestellt werden. Zudem sollte ein IT-Sicherheitsbeauftragter eingesetzt werden, der die IT-Sicherheitsleitlinien auf betrieblicher Ebene durchsetzt und als Ansprechpartner für das Thema IT-Sicherheit nach außen fungiert.

Das BSI stellt auf seiner Webseite www.bsi.bund.de frei zugängliche Publikationen wie die BSI-Standards zum IT-Sicherheitsmanagement bereit. Dort sind auch die IT-Grundschutzkataloge des BSI abrufbar, in denen eine einfache Methode dargestellt wird, nötige IT-Sicherheitsmaßnahmen zu identifizieren und umzusetzen. Mit der Zertifizierung nach ISO 27001 auf Basis von IT-Grundschutz können Unternehmen ihr IT-Sicherheitsmanagement sowie konkrete IT-Sicherheitsmaßnahmen überprüfen und von neutraler Stelle bestätigen lassen.

Eine weitere Möglichkeit, Transparenz hinsichtlich der Sicherheitseigenschaften von IT-Produkten zu schaffen, ist die Prüfung und Bewertung von IT-Produkten und -Systemen nach einheitlichen Standards. Beim Einsatz von IT-Produkten mit Sicherheitseigenschaften sollte daher auf zertifizierte IT-Produkte nach dem international anerkannten Standard der Common Criteria (CC) oder den europäischen ITSEC (Information Technology Security Evaluation Criteria) zurückgegriffen werden.

Verantwortliche in Unternehmen können sich auf der BSI-Webseite zudem in zwei Mailinglisten eintragen, über die vor neuen Computer-Viren, Würmern und anderen Schadprogrammen gewarnt sowie über neue Sicherheitslücken und Schwachstellen in IT-Systemen informiert wird.

Kritische Infrastrukturen

Im Umsetzungsplan KRITIS (UP KRITIS, vgl. Kapitel 3.2.) werden im Jahr 2007 erstmalig die Eckpunkte der künftigen Zusammenarbeit zur IT-Sicherheit zwischen den Betreibern Kritischer Infrastrukturen festgelegt. Der Schwerpunkt der Aktivitäten liegt dabei im Bereich der Prävention und der Reaktion auf IT-Krisen. Durch ein umfassendes, gemeinsam generiertes Lagebild sollen diese frühzeitig erkannt werden. Abgestimmte und eingeübte Prozesse sollen die Auswirkungen solcher Vorfälle minimieren.

In den nächsten Monaten sollen diese Prozesse in enger Zusammenarbeit zwischen dem BSI und den Betreibern Kritischer Infrastrukturen definiert werden. Der bereits in ersten Ansätzen vorhandene Informationsaustausch zu IT-Sicherheitsvorfällen wird weiter ausgebaut. Langfristig sollen alle Informationen, die für ein IT-Lagebild relevant sind, im IT-Lagezentrum des BSI zusammenfließen und in aussagekräftiger Form aufbereitet werden.

7.3 Verwaltung

Mit dem Umsetzungsplan Bund (UP Bund) wird im Jahr 2007 erstmalig eine einheitliche IT-Sicherheitsleitlinie für sämtliche Bundesressorts erarbeitet. Sie wird technische, organisatorische und prozessuale Standards für die Bundesverwaltung festschreiben. In allen Behörden der Bundesverwaltung werden angemessene IT-Sicherheitsmaßnahmen realisiert. Zentrale Betätigungsfelder sind außerdem:

Zusammenarbeit bei IT-Krisen

Im Lagezentrum des BSI wird die nationale IT-Lage im 8/7-Betrieb beobachtet. Bei Lageverschärfungen können so frühzeitig Bundesbehörden und andere Partner gewarnt oder alarmiert werden. Bei sich abzeichnenden IT-Krisen wird dieses Lagezentrum zum IT-Krisenreaktionszentrum des Bundes. So kann die gesamte IT-Sicherheitskompetenz des BSI eingesetzt werden, um behördenübergreifend die Auswirkungen solcher IT-Krisen zu minimieren.

Sicherheit von Kommunikationsinfrastrukturen

Genauso wie in der Wirtschaft sind für die öffentliche Verwaltung E-Mail, der Dokumentenaustausch oder elektronische Transaktionen über das Internet bzw. Behördennetze zum Alltag geworden. Es ist davon auszugehen, dass der

elektronische Datenaustausch zwischen Behörden und zu Bürgern und Wirtschaft in den nächsten Jahren weiterhin quantitativ und qualitativ erheblich zunehmen wird.

Grundlage der Behördenkommunikation sind zuverlässige und sichere Netzinfrastrukturen. Diese müssen besonders geschützt werden, da bei einem Ausfall die Arbeitsfähigkeit der öffentlichen Verwaltung erheblich eingeschränkt wäre. In Anbetracht der Bedrohungslage sind in den vergangenen Jahren die bedeutendsten Netzinfrastrukturen der Bundesverwaltung, der Informationsverbund Berlin-Bonn (IVBB) und der Informationsverbund der Bundesverwaltung (IVBV) weiterentwickelt worden. So wird eine sichere und verfügbare Behördenkommunikation gewährleistet.

Stetig wachsende Bedrohungen, neue Anforderungen der Bundesverwaltung (zum Beispiel gesetzliche Vorgaben) und neue technische Entwicklungen erfordern eine Neustrukturierung und Weiterentwicklung der Netzinfrastrukturen.

Insbesondere muss die Sicherheit der Behördenkommunikation zwischen Bund, Ländern und Kommunen verbessert werden. Im Jahr 2006 wurde daher im Rahmen des Aktionsplans Deutschland-Online der Aus- und Aufbau einer integrierten, sicheren Kommunikationsinfrastruktur für die deutsche Verwaltung in Bund, Ländern und Gemeinden (KIVD) beschlossen. Die Notwendigkeit sicherer Netzinfrastrukturen wurde auch als ein Ergebnis des IT-Gipfels im Kanzleramt formuliert.

Aufklärung und Schulung

Für IT-Sicherheitsbeauftragte in Behörden wurde an der Bundesakademie für die öffentliche Verwaltung (BAköV) eine mehrwöchige Schulungsreihe eingerichtet. Das IT-Sicherheitsniveau in der Bundesverwaltung soll so weiter verbessert und angeglichen werden.

7.4 Gemeinschaftliches Handeln

Frühwarnung

Zusammen mit Partnern aus der Forschung und der Wirtschaft fördert das BSI mehrere Projekte zum Aufbau eines „Nationalen IT-Frühwarnsystems“. Das Ziel: Alle potenziell Betroffenen sollen zu einem möglichst frühen Zeitpunkt

schnell und umfassend über drohende Sicherheitsvorfälle informiert werden, um die rasche Einleitung von Gegenmaßnahmen zu ermöglichen.

Für die Beobachtung, Analyse und Bewertung von IT-Sicherheitsvorfällen wurde durch das BSI ein Sensornetzwerk eingerichtet. Weitere Informationen für die Beurteilung der IT-Sicherheitslage werden durch die Kooperation mit anderen nationalen und internationalen IT-Sicherheitsteams und Partnerbehörden, Betreibern von Netzwerken sowie Herstellern von IT-Produkten gewonnen. Von der Bundesregierung wurde außerdem der Ausbau eines internationalen Watch-and-Warning-Netzwerks mit initiiert. Informationen zu aktuellen Bedrohungen und Risiken werden den potenziell Betroffenen zielgruppengerecht über verschiedene Warn- und Informationsdienste bereitgestellt und durch konkrete Handlungsempfehlungen ergänzt. Dadurch haben alle Personen, die Verantwortung für IT-Systeme und Informationsinfrastrukturen tragen, Zugriff auf geeignete Informationsangebote – von der Privatperson bis zum Verantwortlichen für die IT in Unternehmen, Behörden oder anderen Organisationen.

Deutschland sicher im Netz e.V.

Die Nutzung von Informationstechnologien und -diensten ist Teil des Alltags sowohl von Unternehmen aller Größen als auch von Privatpersonen geworden. Der im Dezember 2006 gegründete Verein „Deutschland sicher im Netz e.V." stellt eine übergreifende und auf Dauer angelegte Plattform für Fragen der Sensibilisierung und Aufklärung rund um IT- und Internetsicherheit dar. Schwerpunkte der zukünftigen Arbeit bilden dabei private Nutzer, gerade auch Computer-Neulinge, sowie kleine und mittelständische Unternehmen, weil hier in besonderem Maße Aufklärungs- und Informationsbedarf besteht. Die operative Aufgabe des Vereins liegt insbesondere in der Stärkung des Bewusstseins für IT- und Internetsicherheit durch Aufklären, Informieren, Sensibilisieren und das Bereitstellen von Handlungsanweisungen. Das Bundesinnenministerium und das BSI unterstützen diese Plattform.

Aktivitäten auf europäischer Ebene

IT-Sicherheit hat längst eine europäische Dimension erhalten. Die IT-Sicherheitssituation in einem Land beeinflusst unweigerlich die Lage der IT-Sicherheit der anderen Länder. Die Bundesrepublik engagiert sich deshalb auch im europäischen Kontext.

Im Jahr 2004 wurde von der Europäischen Gemeinschaft die Europäische Agentur für Netz- und Informationssicherheit (ENISA) eingerichtet. Die ENISA hat die Aufgabe, einen Beitrag zu einem hohen Niveau der IT-Sicherheit in der Gemeinschaft zu leisten und die Entstehung einer Kultur der Netz- und Informationssicherheit zugunsten der Bürger, Verbraucher, Unternehmen und der öffentlichen Verwaltung zu fördern. Deutschland hat sich intensiv um die Einrichtung der Agentur bemüht und unterstützt deren Arbeit, zum Beispiel durch die Leitung einer Arbeitsgruppe mit dem Ziel der Förderung von IT-Sicherheitsmanagement in Europa.
2006 wurde die Strategie der Kommission für die sichere Informationsgesellschaft verabschiedet. Sie beschreibt, wie eine kohärente, ganzheitliche Vorgehensweise im Bereich der Netz- und Informationssicherheit gefördert werden soll. Diese Mitteilungen und weitere Regelwerke werden immer stärkeren Einfluss auf die IT- Sicherheitslandschaft und die Lage der IT-Sicherheit in Deutschland haben. Die IT-Sicherheit ist daher Thema mehrerer Veranstaltungen der Deutschen EU-Ratspräsidentschaft 2007.

Neben der aktiven Mitarbeit im Rahmen der Europäischen Union ist auch die zwischenstaatliche und multilaterale Zusammenarbeit von großer Bedeutung:

European Government CERTs-Gruppe (EGC)

Eine besonders erfolgreiche Kooperation auf europäischer Ebene ist die European Government CERTs-Gruppe (EGC). Sie ist ein informeller Zusammenschluss von Computer-Notfallteams (englisch Computer Emergency Response Teams, CERTs) europäischer Behörden. Ihr Ziel ist die Entwicklung einer effektiven Kooperation in Bezug auf IT-Sicherheitsvorfälle (englisch Incident Response). Ausgangspunkte des gemeinsamen Handelns sind dabei gleichartige Interessen der Mitglieder aufgrund ähnlicher Zielgruppenstrukturen und Problemlagen. Um dieses Ziel zu erreichen, entwickeln die Mitglieder der EGC-Gruppe gemeinsame Maßnahmen gegen großflächige oder regionale IT-Sicherheitsvorfälle in Netzwerken und tauschen Informationen über IT-Sicherheitsvorfälle, Gefährdungspotenziale und Schwachstellen aus. Fachwissen und Expertise einzelner Personen wird in der Gruppe weitergegeben und die Gründung von Behörden-CERTs innerhalb der europäischen Staaten angeregt und voran getrieben.
Derzeit arbeiten neben dem Computernotfallteam des Bundes (CERT-Bund) sieben weitere europäische CERTs in der EGC-Gruppe mit.

Trusted Computing

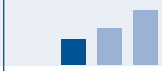
Das BSI führt im Bereich Trusted Computing gemeinschaftlich mit anderen Behörden, Industrieunternehmen und Universitäten Projekte und Veranstaltungen durch. Dabei soll ein Bewusstsein für Einsatzmöglichkeiten und Gefahren dieser neuen Technologie geschaffen werden. Auch auf europäischer Ebene arbeitet das BSI eng mit Behörden und der EU-Kommission zusammen, um Know-how zu bündeln und Forschungsaktivitäten zu forcieren. Beispiel dafür ist eine „Summerschool" zum Thema Trusted Infrastructure, die im Jahr 2006 zum ersten Mal in Großbritannien stattgefunden hat und 2007 in Deutschland durchgeführt wird. Hierbei treffen sich Wissenschaftler aus verschiedenen europäischen Ländern, um Forschungsaktivitäten zu bündeln.

Fazit

8 Fazit

Die Technisierung nimmt zu, immer mehr geschäftliche und private Aktivitäten werden in die virtuelle Welt verlagert. Gleichzeitig ist auch weiterhin die Tendenz zur Professionalisierung der IT-Bedrohungen festzustellen.

Gefährdungstrends

Bedrohung	2005	2007	Prognose
Zero-Day-Exploits			
Trojanische Pferde			
Viren			
Würmer			
Spyware/Adware			
DDos-Angriffe			
Unerwünschte E-Mails			
Bot-Netze			
Phishing			
Identitätsdiebstahl/Social Engineering			
Dialer			
Ping-Anrufe			
Innentäter			

 Gefährdung nimmt zu gleichbleibende Gefährdung Gefährdung sinkt

Quelle: BSI

Abbildung 13: Entwicklung von IT-Bedrohungen nach Einschätzung des BSI [3]

Risikopotenzial innovativer Technologien

Technologie	2005	2007	Prognose
Voice over IP (VoIP)			
Wireless LAN (WLAN)			
Handy/PDA			
Asynchrones Javasript und XML (AJAX)			
Prozesssteuerungssysteme (SCADA)			
RFID			

 Gefährdung nimmt zu

 gleichbleibende Gefährdung

 Gefährdung sinkt

Quelle: BSI

Abbildung 14: Risikopotenzial innovativer Technologien nach Einschätzung des BSI [3]

Diese Tabellen stellen die Entwicklung der Gefährdung durch IT-Bedrohungen und des Risikopotenzials innovativer Technologien sowie deren prognostizierte Tendenz dar. Dabei zeigen sich deutliche Veränderungen seit dem erstmaligen Erscheinen des Lageberichts im Jahre 2005. Wie sich die Bedrohungslage tatsächlich entwickelt, ist schwer vorhersehbar. Der Sicherheit dienlichen Maßnahmen auf Seiten der Hersteller, Administratoren und auch der Behörden stehen kontinuierlich veränderte und angepasste Methoden von Angreifern gegenüber. Mit zunehmender Verbreitung einer Technologie steigt zudem auch das Gefährdungspotenzial. Daher ist langfristig nicht mit einer Entspannung der IT-Sicherheitslage zu rechnen. Es erfordert einen immer größeren Aufwand, die Risiken auf ein tragbares Maß zu beschränken und Vertraulichkeit, Verfügbarkeit und Integrität von Informationen sicher zu stellen.

Handlungsbedarf besteht dabei auf zwei Seiten. Die technische Funktionsweise von informationstechnischen Produkten und Systemen ist für weite Kreise der Anwender nicht durchschaubar. Anbieter sind daher in der Pflicht, dem Thema IT-Sicherheit eine hohe Priorität zuzuweisen und zum Beispiel durch einheitliche Prüfung und Zertifizierung der Produkte eine Transparenz hinsichtlich der Sicherheitseigenschaften von IT-Produkten zu schaffen. Eine Integration möglichst automatisierter Sicherheitsmechanismen von vornherein, die die vom

Anwender notwendige zusätzliche Interaktion auf ein Minimum beschränkt, könnte das Sicherheitsniveau weiter erhöhen und das Risikopotenzial reduzieren.

Allerdings beschränkt sich notwendiges Handeln nicht nur auf die Hersteller und entsprechende staatliche Stellen, die sich mit der Lage der IT-Sicherheit in Deutschland befassen. Sie können keinen hundertprozentigen Schutz bieten. Je perfider und schneller die Angreifer werden, desto mehr müssen daher auch die Anwender aktiv werden.

Der beste Schutz der Anwender in Gesellschaft, Wirtschaft und Verwaltung ist durch eine Stärkung ihrer IT-Sicherheitskompetenz zu erreichen. Sie ist ein wesentlicher Bestandteil, um die Rahmenbedingungen für den sicheren Einsatz von IT zu verbessern. Es muss Interesse dafür geweckt werden, sich dauerhaft und aktuell über neue Risiken zu informieren und den Empfehlungen wirkungsvoller Sicherheitsmaßnahmen zu folgen. Das Verhalten der Nutzer muss von Wachsamkeit geprägt sein, sie müssen sich ihrer Eigenverantwortung bewusst sein. Das Installieren von Sicherheitsupdates und Patches sollte in Zukunft ebenso selbstverständlich werden, wie der Griff zum Sicherheitsgurt im Auto.

Auch wenn der vorliegende Bericht einigen Gruppen ein gesteigertes Bewusstsein für IT-Gefahren attestiert, besteht doch weiterhin Verbesserungspotenzial. So trifft man etwa in Unternehmenskreisen auch heute noch oftmals auf das Argument, Sicherheitsmaßnahmen müssten bei knappen finanziellen Mitteln eingespart werden. Dies ist ein gefährlicher Trugschluss. Schäden, die beispielsweise durch Systemzusammenbrüche oder Spionageangriffe entstehen, können rasch ein Vielfaches der Sicherheitsinvestitionen betragen. Letztlich zahlt sich Sicherheit immer aus, für Anwender aus allen Bereichen ebenso wie für die gesamte Gesellschaft. Sie gehört zu der Art von Versicherungen, die jeder haben muss.

9 Quellen

[1] Informations- und Kommunikationstechnologie in privaten Haushalten 2006, Statistisches Bundesamt, Wiesbaden 2007.

[2] BSI: Die Lage der IT-Sicherheit in Deutschland 2005.

[3] BSI-Erhebungen.

[4] Capgemini: IT-Trends 2006, http://www.de.capgemini.com/m/de/tl/IT-Trends_2006.pdf.

[5] InformationWeek: IT-Security 2006.

[6] kes/Microsoft-Sicherheitsstudie: Lagebericht zur Informations-Sicherheit 2006, http://www.kes.info/archiv/material/studie2006.

[7] X-Force Threat Inside Quarterly Q406 (Januar 2007), http://documents.iss.net/ThreatIQ/ISS_XFTIQ_Q406.pdf.

[8] Symantec Internet Security Threat Report, Volume X (September 2006), http://www.symantec.com/region/de/deresc/download/Symantec_ISTR_X_I-06.pdf.

[9] Symantec Internet Security Threat Report, Volume IX (März 2006) und Volume VIII (September 2005), Download nach Registrierung unter: http://www4.symantec.com/Vrt/offer?a_id=22651 und http://www4.symantec.com/Vrt/offer?a_id=20262.

[10] Institut für Internetsicherheit der FH Gelsenkirchen: Online-Umfrage zur E-Mail-Verlässlichkeit 2006, http://www.internet-sicherheit.de/projekte-email.html.

[11] ENISA: Study on security and countermeasures against spam, 2006, http://www.enisa.europa.eu/doc/pdf/deliverables/enisa_security_spam.pdf.

[12] McAfee-Studie, „Gefahren von innen“, 2005.

[13] BITKOM Presseinformation vom 16. Oktober 2006, http://www.bitkom.org/de/presse/8477_42026.aspx.

[14] Wirtschaftsrechnungen (Fachserie 15, Reihe 2) - Ausstattung privater Haushalte mit langlebigen Gebrauchsgütern 2000-2006, Statistisches Bundesamt, Wiesbaden 2007.

[15] Gartner, Hype Cycle for Cyberthreats 2006.

[16] Deloitte, Sicherheitsstudie 2006.

[17] BITKOM Presseinformation vom 5. November 2006, http://www.bitkom.de/de/presse/8477_42419.aspx.

[18] eBusiness-Barometer 2006/2007, http://www.wegweiser.de/01_beschaffen/x01-d13-a.htm.

[19] Eurostat-Erhebungen 2006, http://epp.eurostat.ec.europa.eu.

[20] ARD/ZDF-Online-Studien 2004-2006.

[21] (N)ONLINER Atlas 2006, TNS Infratest Holding GmbH & Co. KG und Initiative D21 (Hrsg.).

10 Glossar

Bluetooth-Stacks
Bluetooth bezeichnet einen Funkstandard für Sprach- und Datenkommunikation. Bluetooth-Stacks sind Schnittstellen, über die Bluetooth-fähige Geräte programmiert werden können.

Business Continuity
Die Fähigkeit einer Organisation, auch nach schwerwiegenden krisenhaften Ereignissen wie beispielsweise dem Zusammenbruch eines IT-Systems weiter zu funktionieren.

CERT
Kurzbezeichnung für „Computer Emergency Response Team". Darunter versteht man Arbeitsgruppen oder Organisationen, die aktive Unterstützung bei IT-Sicherheitsproblemen bieten. Ein Beispiel dafür ist das Computer Emergency Response Team für Bundesbehörden (CERT-Bund) des BSI.

Exploit
Ausnutzung einer Schwachstelle in einem Softwareprogramm.

ECC (Elliptic Curve Cryptography)
Verschlüsselungsverfahren, das eine geringere Rechenleistung als z.B. RSA sowie kürzere Schlüssellängen benötigt. ECC wird in Zukunft vermutlich insbesondere bei Chipkarten verstärkt zum Einsatz kommen.

Hashwert
Eine kryptographische Hashfunktion errechnet z.B. aus einer Datei beliebiger Länge einen Bitstring fester Länge. Ein Hashwert wird auch als fingerprint bezeichnet. Die Zielsetzung: Es soll praktisch nicht möglich sein, zwei unterschiedliche Dateien angeben zu können, die denselben Hashwert besitzen.

HBCI (Home Banking Computer Interface)
Standard zur Absicherung von Online-Banking. HBCI besteht meist in der Nutzung einer HBCI-Chipkarte mit einem Chipkartenleser, der die sichere PIN-Eingabe unterstützt.

iTAN
Indiziertes TAN-Verfahren; bei iTAN muss eine bestimmte TAN der Liste eingegeben werden. Diese ist an einen bestimmten Auftrag gebunden und kann nicht beliebig verwendet werden.

mTAN (auch smsTAN)
Mobile TAN oder smsTAN. Nach erfolgreicher Online-Übermittlung einer Überweisung an ein Geldinstitut sendet dieses eine TAN per SMS auf das Handy des Nutzers. Mit der Eingabe dieser TAN, die nur für diesen Vorgang gültig ist, wird der Online-Banking-Vorgang am Computer abgeschlossen.

Phishing
Ein Kunstwort, das sich aus „password“ und „fishing“ zusammensetzt. Es bezeichnet eine Methode, um mithilfe gefälschter E-Mails an vertrauliche Daten zu gelangen. Zunehmend werden dafür auch Trojanische Pferde eingesetzt.

Quantencomputer
Quantencomputer basieren auf einer völlig neuartigen Technik und können Aufgaben wesentlich schneller als konventionelle Computer durchführen. Ihre Entwicklung steht noch am Anfang, derzeit existierende Quantencomputer haben nur sehr geringe Kapazitäten.

Quantenkryptographie
Die Quantenkryptographie nutzt charakteristische Eigenschaften der Quantenmechanik, um einen sicheren Schlüsselaustausch zwischen zwei Parteien zu initiieren. Im Gegensatz zu klassischen Schlüsselaustauschverfahren kann der Empfänger erkennen, wenn ein Dritter auf der Übertragungsstrecke versucht hat, die übertragene Information in Erfahrung zu bringen.

RFID (Radio Frequency Identification)
Verfahren zur automatischen Identifizierung von Objekten über Funk. Ein RFID-System besteht aus einem Transponder und einem Lesegerät: Das Lesegerät liest die Daten vom Transponder und weist ggf. den Transponder an, weitere Daten zu speichern. Die Reichweite liegt je nach Anwendungsfall im Zentimeter- oder Meterbereich.

RSA-Verfahren
Vor allem im Bereich der digitalen Signatur weit verbreitetes kryptologisches Verfahren.

SCADA- und Prozesssteuerungssysteme
SCADA- und Prozesssteuerungssysteme werden zur Überwachung und Steuerung komplexer technischer Prozesse beispielsweise in der Produktion und Verarbeitung materieller Güter, der Stromerzeugung oder der Wasserversorgung eingesetzt. Die Steuerungssysteme bestehen zu einem wesentlichen Teil aus spezieller Informationstechnik.

Social Engineering
Im Zusammenhang mit IT-Sicherheit wird der Begriff für eine Strategie von Online-Betrügern gebraucht. Indem sie individuell auf ihre Opfer zugehen, steigern sie ihre Erfolgsraten: Zuvor ausspionierte Daten wie etwa Surfgewohnheiten oder Namen aus dem persönlichen Umfeld des Opfers werden dazu verwandt, beispielsweise Phishing-E-Mails persönlich zu formulieren und dadurch Vertrauen zu erwecken.

Web 2.0
Web 2.0 steht für die Fortentwicklung des Web zu einer Plattform von Services, die jeder Einzelne beeinflussen, verändern und individuell weiter verwenden kann. Beispiele sind Wikis, Blogs oder interaktive Bildergalerien.

Herausgeber
Bundesamt für Sicherheit in der Informationstechnik (BSI)
53175 Bonn

Texte und Redaktion
Bundesamt für Sicherheit in der Informationstechnik
pressto – Agentur für Medienkommunikation, Köln

Layout und Gestaltung
plankundplank design, Köln

Druck
Druckhaus Brümmer, Alfter

Stand
April 2007

Bezugsstelle
Bundesamt für Sicherheit in der Informationstechnik
Referat 321 – Information, Kommunikation, Öffentlichkeitsarbeit
Godesberger Allee 185 - 189
53175 Bonn
Tel.: +49 228 99 9582-0
E-Mail: oeffentlichkeitsarbeit@bsi.bund.de
Internet: www.bsi.bund.de