Bundesamt
für Sicherheit in der
Informationstechnik

Die Lage der IT-Sicherheit in Deutschland 2005

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

Inhaltsverzeichnis

Abbildungsverzeichnis

Vorwort

1 Vorwort

Wirtschaft und Gesellschaft sind auf eine sichere Informationstechnik angewiesen. Zu groß ist die Vernetzung, zu groß ist die Abhängigkeit von funktionierender Informationstechnik inzwischen geworden. IT-Sicherheit ist Teil der Inneren Sicherheit und muss daher als nationale Aufgabe verstanden werden.

Mit dem Bundesamt für Sicherheit in der Informationstechnik (BSI) verfügt Deutschland über eine spezialisierte Fachbehörde für alle Fragen rund um die IT-Sicherheit. Das Ziel des BSI: der sichere Einsatz von Informations- und Kommunikationstechnik in unserer Gesellschaft. Dazu ist es notwendig, die gegenwärtige Situation zu erfassen, zu analysieren und der Öffentlichkeit vorzustellen.

Dieser Bericht stellt die aktuelle Lage der IT-Sicherheit in Deutschland dar. Er gibt einen Überblick über die anstehenden Herausforderungen. Zudem zeigt der Bericht Trends auf und ermöglicht deren Einordnung und Bewertung. Denn nur wer die Gefahren genau kennt, kann angemessen handeln. Wir werden nur dann weiterhin die Vorteile der Informationstechnik und deren weltweite Vernetzung uneingeschränkt nutzen können, wenn wir diese entsprechend schützen und damit auch uns selbst.

Juli 2005

Dr. Udo Helmbrecht

Präsident des BSI

Einleitung

2 Einleitung

Informationstechnik (IT) ist zu dem herausragenden gesellschaftlichen Faktor unserer Zeit geworden. Weltweit steigt die Nutzung und damit auch die Abhängigkeit von IT – Deutschland stellt hier keine Ausnahme dar. Computer, Mobiltelefon und Internet haben sich zur Grundlage der mobilen, wissensbasierten und vernetzten Informationsgesellschaft entwickelt.

Der Wandel der Informationstechnik hat zu neuen Bedrohungsformen geführt. Deutlich wird dies am Beispiel von Schadprogrammen. Gelangten Computerviren und -würmer früher über den Austausch infizierter Disketten in Umlauf, verbreiten sich diese heute über Internet und E-Mail. Die neuen Verbreitungswege erhöhen die Schlagkraft dieser Schädlinge. Angesichts der Vernetzung von IT-Systemen kommt es in kürzester Zeit zu globalen Epidemien mit enormen finanziellen Auswirkungen auf die Gesellschaft.

Mit diesem Bericht informiert das BSI über die Lage der IT-Sicherheit in Deutschland. Die Beschreibung aktueller technologischer Sicherheitslücken und Bedrohungen verdeutlicht, welche Gefahren beim Einsatz von IT heute berücksichtigt werden müssen. Zudem zeigt der Bericht, in welche Richtung sich die Bedrohungen entwickeln und welche Vorkehrungen getroffen werden müssen, um Gefahren auch in Zukunft abwehren zu können.

Die Ausführungen verdeutlichen, dass alle gesellschaftlichen Gruppen einer besonderen Verpflichtung zur Gewährleistung der Sicherheit unterliegen. Um angemessene IT-Sicherheit zu realisieren, müssen Verwaltung, Wirtschaft sowie Bürgerinnen und Bürger dem Thema einen zentralen Stellenwert einräumen. Da jede Gruppe Informationstechnik unterschiedlich nutzt, unterscheiden sich auch die jeweiligen Anforderungen an die IT-Sicherheit. Der Bericht zeigt zielgruppenspezifisch die umfassenden Aufgaben auf, mit denen sichere und zuverlässige IT gewährleistet wird.

Der Bericht fasst Erkenntnisse aus eigenen Erhebungen und Fachkontakten zusammen. Ergänzt und verifiziert werden diese durch Studien verschiedener IT-Sicherheitsunternehmen.

IT-Sicherheits-bewusstsein und IT-Sicherheitskompetenz in der Gesellschaft

3 IT-Sicherheitsbewusstsein und IT-Sicherheitskompetenz in der Gesellschaft

IT-Sicherheitsbewusstsein umfasst verschiedene Bereiche: Kenntnisse über die Bedeutung von IT-Sicherheit gehören ebenso dazu wie das Verständnis des jeweils angemessenen IT-Sicherheitsniveaus und der eigenen Verantwortlichkeiten. Erst wenn beides vorhanden ist, kann von einer dezidierten IT-Sicherheitskompetenz gesprochen werden.

Studien belegen, dass IT-Sicherheitskompetenz in den gesellschaftlichen Gruppen kaum verbreitet ist. Obwohl Bürgerinnen und Bürger zunehmend von Informationstechnik abhängen – sei es am Arbeitsplatz, beim digitalen Zahlungsverkehr, in der Kommunikation oder im E-Commerce – räumen nur wenige sicherer Informationstechnik in der Praxis den erforderlichen Stellenwert ein. Ähnliches gilt für Wirtschaft und Staat. In den Unternehmen wird das Thema Sicherheit zu oft erst nach einem Schadensfall ernst genommen. Und das, obwohl wirtschaftlicher Erfolg und Konkurrenzfähigkeit heute maßgeblich von funktionierender IT bestimmt werden. Auch für die Verwaltung stellt zuverlässige Informationstechnik die Basis für die täglichen Arbeitsabläufe dar. Und doch fehlt es hier weithin am erforderlichen Sicherheitsbewusstsein.

3.1 Bürgerinnen und Bürger

Die deutschen Internetnutzer verfügen nach eigenen Angaben über gute IT-Fachkenntnisse: Nach einer repräsentativen Studie des BSI kennt sich die Hälfte gut bis sehr gut aus [2]. Nur jeder Zehnte gibt an, wenige bis gar keine Fachkenntnisse zu besitzen. Hoch ist in der Bevölkerung auch das Wissen über Angriffsmöglichkeiten, die durch die Verbindung mit dem Internet bestehen. 90 Prozent ist bekannt, dass der eigene Computer von Fremden missbraucht werden kann. Und sieben von zehn Nutzern sind sich im Klaren darüber, dass die Absenderadressen von E-Mails gefälscht sein können [2].

Trotz dieser vermeintlich positiven Ergebnisse zeigt die Studie auch, dass das Thema IT-Sicherheit in der Praxis eine untergeordnete Rolle spielt. Jeder vierte

Nutzer verzichtet auf ein Virenschutzprogramm und nur die Hälfte setzt eine Firewall ein. Datensicherungen nimmt ebenfalls nur jeder Zweite regelmäßig vor. Auch der Schutz des Systems durch die Installation von aktuellen Sicherheitsupdates für Betriebssystem und Anwendungen wird vernachlässigt. Nur jeder dritte Anwender installiert regelmäßig Updates zum Schließen von Sicherheitslücken. Um das Aktualisieren der Antivirensoftware kümmern sich vier von fünf Nutzern einmal im Monat, jeder Dritte wöchentlich.

3.2 Wirtschaft

Für IT-Verantwortliche in der Wirtschaft ist IT-Sicherheit eines der wichtigsten Themen. 83 Prozent der Befragten setzt das Thema auf Platz eins oder zwei der Prioritätenliste [7].

In Deutschland sehen 89 Prozent der IT-Verantwortlichen die Wirtschaft durch mangelnde IT-Sicherheit gefährdet. Gefragt nach der Einschätzung der Sicherheitslage ihrer eigenen Organisation, gibt allerdings nur knapp ein Viertel an, akut bedroht zu sein [3]. Die Verbreitung von Schadprogrammen stellt für die Mehrheit die eindeutig größte Gefahr für die IT-Sicherheit des eigenen Unternehmens dar. Allerdings nimmt hier der Faktor Mensch – also Irrtum und Nachlässigkeit eigener Mitarbeiter – in der Wahrnehmung von IT-Sicherheit ebenfalls einen hohen Stellenwert ein [9]. Hinzu kommen die Erweiterung herkömmlicher Unternehmensnetze um mobile Computer wie Notebooks oder PDAs, die Vernetzung mit Heim- und Telearbeitsplätzen sowie drahtlose Übertragungstechnologien wie WLAN. Diese Bereiche stellen aus Sicht vieler IT-Sicherheitsbeauftragter ein wesentliches und neues Risiko dar.

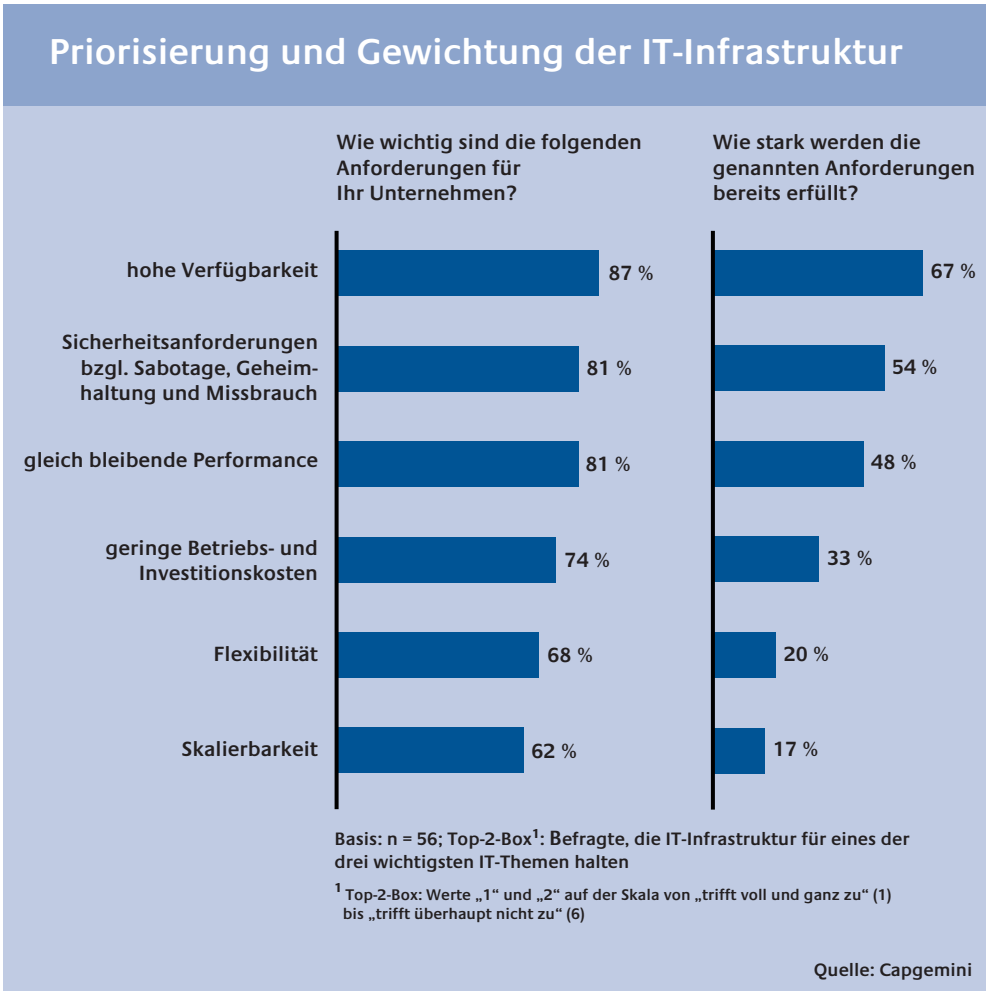

Abbildung 1: Priorisierung und Gewichtung der IT-Infrastruktur in deutschen Unternehmen [7]

Dem Wissen um IT-Sicherheitsprobleme stehen Hindernisse bei der Entwicklung und Umsetzung entsprechender Sicherheitskonzepte gegenüber. Studien zufolge hat nur rund die Hälfte der IT-Verantwortlichen eine schriftlich fixierte Strategie zur Informationssicherheit [11]. Auch unzureichende Finanzmittel werden als Hindernis genannt. Trotz des wachsenden Gefahrenpotenzials stellten 2004 nur 39 Prozent der deutschen Unternehmen ein im Vergleich zum Vorjahr höheres Budget für IT-Sicherheit zur Verfügung, bei 40 Prozent stagnierte der Etat [12].

Gefahrenbereich	Bedeutung heute		Prognose		Schäden	
	Rang	Priorität	Rang	Priorität	Rang	ja, bei
Irrtum und Nachlässigkeit eigener Mitarbeiter	1	1,50	2	1,70	2	51 %
Malware (Viren, Würmer, Trojanische Pferde usw.)	2	1,34	1	2,80	1	54 %
unbefugte Kenntnisnahme, Informationsdiebstahl, Wirtschaftsspionage	3	0,60	4	1,14	8	9 %
Softwaremängel/-defekte	4	0,57	5	0,96	3	43 %
Hacking (Vandalismus, Probing, Missbrauch usw.)	5	0,48	3	1,26	5	9 %
Hardwaremängel/-defekte	6	0,40	8	0,32	4	38 %
unbeabsichtigte Fehler von Externen	7	0,30	9	0,26	7	15 %
höhere Gewalt (Feuer, Wasser usw.)	8	0,24	11	0,04	9	8 %
Manipulation zum Zweck der Bereicherung	9	0,17	7	0,43	10	8 %
Mängel der Dokumentation	10	0,15	10	0,20	6	17 %
Sabotage (inkl. DoS)	11	0,12	6	0,55	11	8 %
Sonstiges	12	0,03	12	0,00	12	3 %

Quelle: kes/Microsoft

Abbildung 2: Bedeutung der verschiedenen Gefahrenbereiche für deutsche Unternehmen [9]

Im Fokus kleiner und mittlerer Unternehmen (KMUs) steht vor allem die zunehmende Bedrohung durch Schadprogramme. Andere Bedrohungen wie Hackerattacken und Spam-Mails spielen dagegen eine noch vergleichsweise geringe Rolle [3].

3.3 Verwaltung

Bei einigen Entscheidungsträgern in der Verwaltung ist die Sensibilität in Bezug auf IT-Sicherheit noch nicht ausreichend. Insbesondere dort, wo die Mitarbeiter nicht ständig mit sicherheitskritischen Vorgängen befasst sind, spielt das Thema IT-Sicherheit eine zu geringe Rolle. Maßnahmen wie Mitarbeiterschulungen und die Bereitstellung entsprechender Informationen griffen bislang zu wenig.

Erschwerend kommt hinzu, dass ausreichend qualifiziertes Fachpersonal für die Betreuung von Informationstechnik nur schwer zu rekrutieren oder zu halten ist. Als Ursache für diesen Umstand werden von den Behörden unter anderem fehlende finanzielle Mittel angegeben.

Schwachstellen und Bedrohungen von IT-Systemen

4 Schwachstellen und Bedrohungen von IT-Systemen

4.1 Sicherheitslücken

Sicherheitslücken in komplexer Software lassen sich nicht völlig vermeiden. Die Qualität einer Software macht sich auch daran fest, wie gut und schnell der Hersteller mit einem Update reagiert und so das Ausnutzen (engl. „Exploit“) der Sicherheitslücke durch ein Schadprogramm verhindert. Zu oft sind jedoch heute die Updates selbst fehlerhaft, beheben nicht die Schwachstelle und ihre Einführung erfolgt zu spät. Aus Unkenntnis der Nutzer, aus Nachlässigkeit oder Zeitknappheit werden zudem verfügbare Updates nicht flächendeckend und zeitnah angewandt. Zwischen Juli und Dezember 2004 wurden mehr als 1.400 neue Schwachstellen entdeckt [15] – ein Anstieg von 13 Prozent im Vergleich zu den vorangegangenen sechs Monaten.

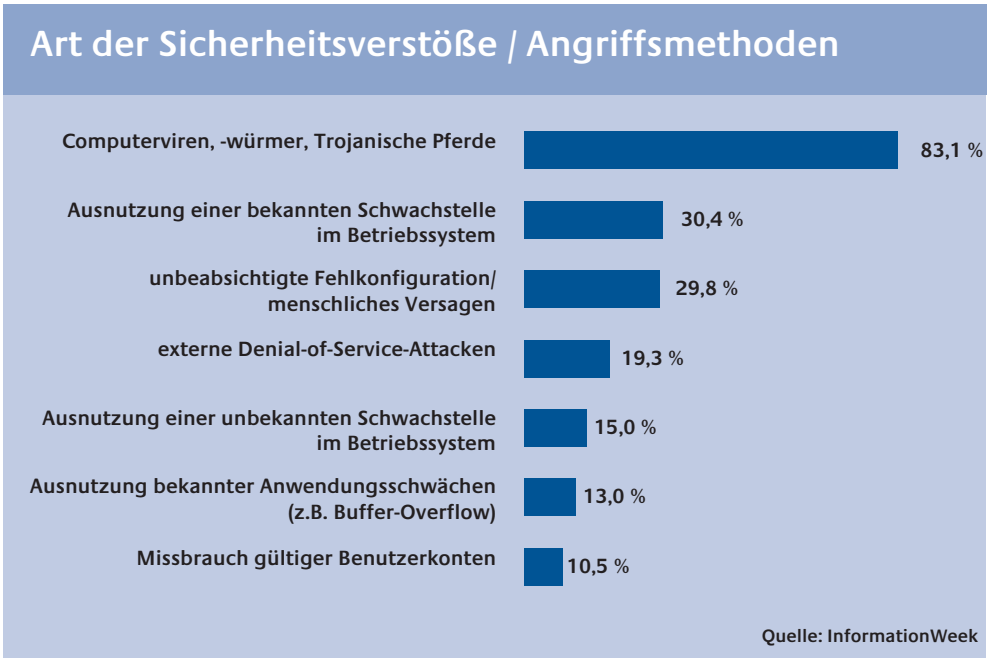

Abbildung 3: Verbreitung von Angriffsmethoden in deutschen und schweizerischen Unternehmen [8]

Die Exploits, mit denen Angreifer die Kontrolle über ein System erlangen, sind über das Internet leicht zugänglich [15]. Laut einer Studie erfolgten im Jahr 2004

etwa 30 Prozent aller Angriffe auf IT-Systeme unter Ausnutzung einer bekannten und 15 Prozent unter Ausnutzung einer noch nicht bekannten Schwachstelle im Betriebssystem. Damit rangieren Exploits auf Platz drei beziehungsweise fünf der verbreitetsten Angriffsmethoden (siehe Abbildung 3). Dennoch will nur jeder zweite IT-Verantwortliche in den kommenden zwölf Monaten der Betriebssystemsicherheit einen größeren Stellenwert einräumen [8].

Der Zeitraum zwischen Bekanntwerden einer Schwachstelle und ihrer Ausnutzung ist bereits heute klein. Durchschnittlich benötigen Angreifer 6,4 Tage, um Methoden zur Übernahme von Systemen zu entwickeln [15].

In dieser kurzen Zeitspanne werden oft weder die notwendigen Programmupdates zur Verfügung gestellt noch Maßnahmen entwickelt, um die Systeme auf andere Weise zu schützen.

Die Zahl so genannter Zero-Day-Exploits nimmt zu. Diese Angriffe sind besonders bedrohlich, da bereits wenige Stunden oder sogar zeitgleich nach Bekanntwerden einer Schwachstelle entsprechende Exploits zum Ausnutzen im Umlauf sind. Den Opfern stehen in diesem kurzen Zeitraum noch keine Updates oder Hinweise zu Gegenmaßnahmen zur Verfügung.

4.2 Schadprogramme

4.2.1 Viren, Würmer, Spyware

Die starke Verbreitung von Standardsoftware und so genannte „Monokulturen“ bei Betriebssystemen gefährden zunehmend die gesamte Informationstechnik. Durch die Dominanz eines einzelnen Produktes am Markt sind die in dem Produkt vorhandenen Schwachstellen besonders weit verbreitet und führen bei Ausnutzung zu hohen Schäden. Angreifer zielen daher mit Schadprogrammen, der am weitesten verbreiteten Angriffsform gegen IT-Systeme, bevorzugt auf Sicherheitslücken dieser Produkte. Hauptquelle für die Verteilung von Computerviren sind insofern arglose Nutzer von Privat- und Unternehmensrechnern.

In der zweiten Hälfte des Jahres 2004 wurden mehr als 7.360 neue Viren- und Wurmvarianten registriert. Das ist eine Zunahme von 64 Prozent gegenüber dem ersten Halbjahr [15].

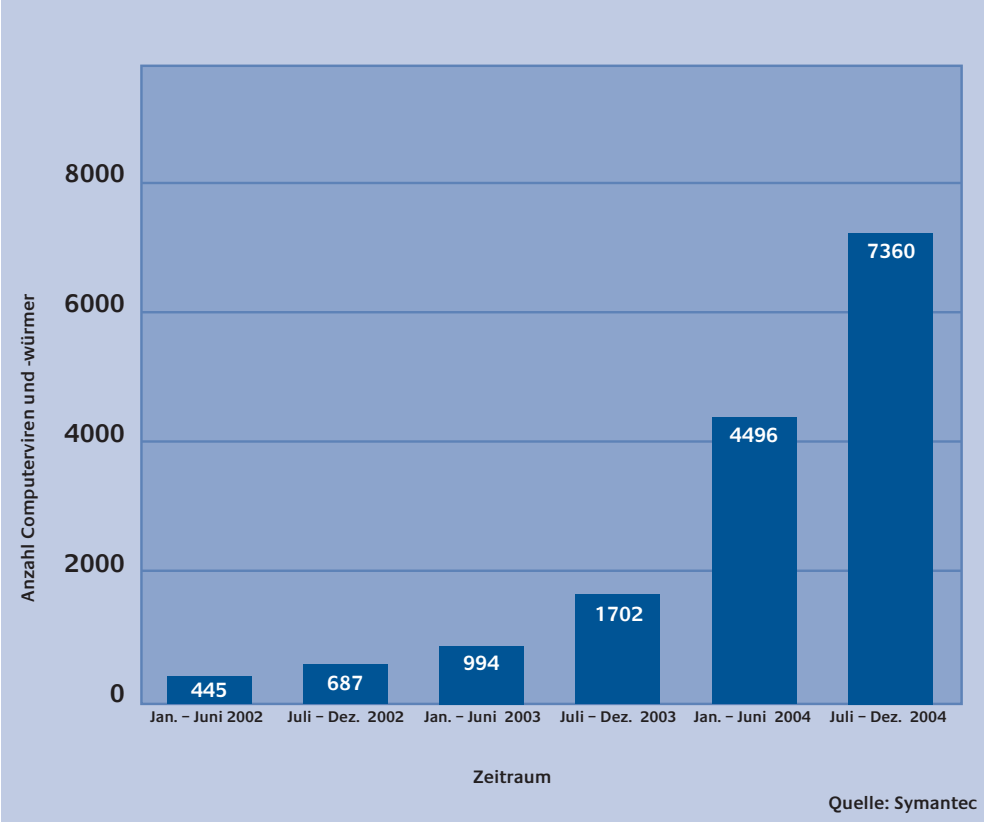

Abbildung 4: Anzahl Computerviren und -würmer weltweit [15]

Acht der zehn häufigsten Exemplare waren Varianten von Massenmailer-Würmern, darunter Netsky, Sober, Beagle und MyDoom. Die Weiterentwicklung von Schadprogrammen zeigt sich an der Variantenvielfalt: Allein 4.300 eigenständige Varianten des Computerwurms Spybot wurden gemeldet. Das entspricht einer Zunahme von 180 Prozent der zu dieser Familie gehörenden Schadprogramme gegenüber den ersten sechs Monaten des Jahres 2004.

An den Netzknotenpunkten des Kommunikationsnetzes der Bundesverwaltung, einer der größten Informationsinfrastrukturen unseres Landes, registrierte das BSI noch nie so viele, so gefährliche und so weit verbreitete Viren wie im Jahr 2004. Durchschnittlich waren monatlich rund 6 Prozent der E-Mails infiziert, die an den zentralen E-Mail-Gateways des Informationsverbundes Berlin-Bonn (IVBB) geprüft wurden. Dabei handelte es sich bei über 80 Prozent der gefundenen Schadprogramme um Computerwürmer und Trojanische Pferde. Die Zahl der registrierten

Schadprogramme in den eingehenden E-Mails nimmt weiterhin zu. Im ersten Quartal 2005 lag der Anteil der infizierten E-Mails bereits bei 8 Prozent.

Das Problem verschärft sich, da Schadprogramme sowohl technisch als auch auf ihre psychologische Wirkung hin immer effektiver programmiert werden. Zu ihrer Verbreitung setzen die Programmierer verstärkt auf die Wirkung des „Social Engineerings“. Sie verleiten Anwender durch eine gezielte und zum Teil personalisierte Ansprache, infizierte Anhänge von E-Mails zu öffnen.

Ein weiterer Trend ist zu beobachten: Computerwürmer werden immer seltener dazu programmiert, direkt irreparable Schäden anzurichten. Vielmehr versuchen Angreifer, den befallenen Rechner für einen kontinuierlichen Missbrauch unter ihre Kontrolle zu bringen. Mit Hilfe Trojanischer Pferde missbrauchen Hacker oft mehrere tausend PCs und vermieten diese so genannten Bot-Netze (vgl. Bot-Netze, S. 21) für kriminelle Zwecke. Sie dienen als Plattform zur Verbreitung neuer Epidemien von Computerschädlingen, für DDoS-Attacken (vgl. DoS-Angriffe, S. 19) und Spamversand (vgl. Spam, S. 20).

Die Zeitabstände zwischen neuen Computervirusepidemien werden kontinuierlich kürzer, da die Autoren von Schadprogrammen vermehrt auf bereits existierende Codes von Computerviren und -würmern zurückgreifen. In Zukunft ist mit Schadprogrammen zu rechnen, die in extrem kurzen Entwicklungszyklen „optimierte“ Varianten nach sich ziehen und sich noch schneller verbreiten.

Darüber hinaus ist Spionagesoftware, so genannte Spyware und Adware, zu einem Sicherheitsrisiko geworden [15]. Diese Programme sammeln ohne Wissen des Computerbesitzers Informationen und geben diese weiter. Spyware kann beispielsweise Tastaturanschläge mitschreiben, Screenshots anfertigen oder E-Mails mitlesen.

Das Gefahrenpotenzial von Spyware und Adware ist unterschiedlich. Gefährliche Spywareversionen fahnden gezielt nach persönlichen Daten wie Passwörtern, Log-in-Daten oder Kontonummern. Adware zeichnet Nutzungsgewohnheiten des Anwenders auf, die anschließend zu Marketingzwecken ausgewertet werden. Zwar richtet diese Art Software keinen direkten Schaden an, sie ist aber unter Aspekten des Datenschutzes bedenklich.

Die Infektion von IT-Systemen durch Spyware geschieht über aktive Inhalte von Webseiten und E-Mails. Da viele Nutzer das Ausführen solcher Inhalte in ihrem

Internetbrowser oder E-Mail-Programm zulassen, ist der Anteil von Reinfektionen durch den mehrfachen Besuch derselben Webseiten hoch. Adware ist zudem vielfach Bestandteil von Software, die im Internet zum kostenlosen Download angeboten wird.

4.2.2 Trojanische Pferde

Trojanische Pferde sind Programme, die neben einer nützlichen offiziellen Funktion eine schädliche nicht dokumentierte Funktion enthalten und diese unabhängig und ohne Wissen des Anwenders ausführen. Im Gegensatz zu Computerviren können sich Trojanische Pferde jedoch nicht selbstständig verbreiten. Durch das unbedachte Ausführen dieser „getarnten" Programme können beträchtliche Schäden für IT-Systeme und entsprechende finanzielle Schäden für die Nutzer entstehen.

Wurden in der Vergangenheit mithilfe Trojanischer Pferde auf infizierten Computern vor allem vertrauliche Daten ausspioniert, ist inzwischen die Kontrolle über den Fremdcomputer das Ziel der Programmierer dieser Schadprogramme. Dazu wird ein so genanntes „Backdoor"-Programm installiert, mit dem der Angreifer den Computer aus dem Internet steuern kann. Im zweiten Halbjahr 2004 machten Trojanische Pferde ein Drittel der 50 häufigsten Internetschädlinge aus [15].

4.3 DoS-Angriffe

Gegen Internetserver gerichtete Angriffe stellen eine Form von Onlinesabotage dar. So genannte DoS-Attacken (engl. „Denial of Service") zielen darauf ab, legitimen Nutzern – beispielsweise Kunden eines Internetshops – den Zugriff auf Dienste zu verwehren. Um dieses Ziel zu erreichen, überflutet der Angreifer den Server mit sinnlosen Datenpaketen und überlastet das System. Je größer die Datenmengen sind, desto effektiver ist der Angriff. Deshalb sind zunehmend verteilte (distributed) Denial-of-Service-Attacken (DDoS) zu registrieren. Bei dieser Angriffsmethode verschaffen sich Angreifer zunächst Ausführungsrechte auf mehreren ungeschützten Computern Dritter. Nachdem auf diesen eine DDoS-Software installiert worden ist, können mithilfe dieser Rechner koordinierte Angriffe gestartet werden.

In Deutschland gaben 15 Prozent der IT-Beauftragten in Unternehmen an, zwischen Ende 2002 und Mai 2004 mit DoS-Angriffen konfrontiert gewesen zu sein [8].

DDoS-Attacken stellen eine ernste Bedrohung für den regulären Betrieb von Webservern dar. Mit den bisher zur Verfügung stehenden Methoden lassen sich DDoS-Angriffe erschweren, ganz ausschalten lassen sich die Gefahren jedoch nicht. Auf dem neuesten Stand der Technik abgesicherte Serversysteme schützen zumindest vor solchen Angriffen, die einen fehlerhaften Programmcode ausnutzen. Internetprovider setzen jedoch zu selten gezielte Schutzmaßnahmen ein, um beispielsweise das Fälschen von IP-Adressen (IP-Spoofing) zu verhindern. Das erschwert die Bekämpfung dieser Angriffsmethode.

4.4 Spam

Neben dem World Wide Web hat sich E-Mail zu einer wichtigen Anwendung des Internets entwickelt. Ein Ausfall dieses Dienstes ist für viele Nutzer nur für kurze Zeit tolerabel. Spam-Mails können Ursache für solche Ausfälle sein. Mittlerweile beträgt der Anteil von Spamnachrichten zwischen 60 und 90 Prozent aller E-Mails [1]. Im Behördennetz IVBB lag die Zahl im Jahr 2004 bei 65 Prozent. Dabei ist eine deutliche Zunahme im Vergleich zum Vorjahr zu erkennen, in dem der Spamanteil noch bei 49 Prozent lag.

Die Versender passen Spam-Mails thematisch zunehmend an aktuelle Anlässe und Feiertage an, um die Adressaten zum Öffnen ihrer Nachrichten zu bewegen. Neben der kommerziellen Spamwerbung werden in Deutschland auch Kettenbriefe (Hoaxes), falsche Viruswarnungen und erstmalig 2004 auch fremdenfeindliche Inhalte verschickt. In der Folge hoher Spamaufkommen kommt es unter anderem zu Arbeitszeitausfällen, zur Überlastung technischer Komponenten oder zu Kosten für den unerwünschten Datenverkehr.

Es ist ein direkter Zusammenhang zwischen Spam und Schadprogrammen erkennbar: Spezielle Massenmailerwürmer suchen auf dem infizierten Computer gespeicherte E-Mail-Adressen, um Spamnachrichten, Computerviren und -würmer dorthin zu versenden. Der massenhafte Versand von Schadprogrammen kann zum Ausbruch regelrechter Epidemien führen.

Trotz des hohen Spamaufkommens werden Antispammaßnahmen in Unternehmen und Verwaltungen in Deutschland noch nicht flächendeckend umgesetzt. Mindestens neun Prozent der Organisationen sind der Spamflut ungeschützt ausgesetzt [1]. In der Rangliste der Verbreitung der Antispammechanismen führen Wort- und Briefkopf-Analyseverfahren (Header-Analyse) vor so genannten schwarzen und weißen Listen, in denen bekannte Spamversender bzw. als sicher geltende Versender aufgelistet sind.

4.5 Bot-Netze

Viele der im Jahr 2004 registrierten Trojanischen Pferde enthalten Funktionen für koordinierte Angriffe gegen Internetserver (vgl. DoS-Angriffe, S. 19). Mit dieser Methode wird die Zahl der von einem Angreifer kontrollierten Computer und damit die Schlagkraft eines verteilten DoS-Angriffs erhöht. Die infizierten Computer bilden so genannte Bot-Netze, die sich jederzeit für Angriffe gegen beliebige Internetserver und so auch zur Erpressung von Unternehmen einsetzen lassen. Auf diese Weise sind Besitzer infizierter Computer nicht mehr nur Opfer, sondern unwissentlich gleichzeitig auch (Mit-)Täter.

Bot-Netze stellen eine besondere Gefahr dar, denn Angreifer sind in der Lage, jederzeit Kontakt zu den infizierten Computern aufzunehmen und unbemerkt weitere Software nachzuladen. So werden beispielsweise nachträglich Programme installiert, die zur Weiterleitung von Spam-Mails über die befallenen PCs genutzt werden.

In den ersten sechs Monaten des Jahres 2004 wurde eine stetige Zunahme von Computern in Bot-Netzen registriert. Die beobachteten Netze bestanden durchschnittlich aus über 30.000 Computern. In der zweiten Jahreshälfte verloren die Netze jedoch rapide an Größe. Zum Ende des Jahres wurden durchschnittlich noch 5.000 infizierte und ferngesteuerte Computer je Bot-Netz gezählt. Der Einschnitt korrespondierte zeitlich mit der Einführung des Windows-XP-Service-Packs 2 [15].

Die Hauptursache für die schnelle Verbreitung von Bot-Netzen liegt in der großen Zahl von Computern mit schnellen und ständig mit dem Netz verbundenen Internetzugängen, bei denen es Nutzern kaum auffällt, wenn auf ihrem PC unkontrollierte Prozesse ablaufen. Zwar minimiert das Einspielen von Sicherheitsupdates

offensichtlich die Gefahr von Bot-Netzen, ein nicht flächendeckender Einsatz adäquater Schutzmaßnahmen verhindert jedoch, dass ihre Ausbreitung generell unterbunden wird.

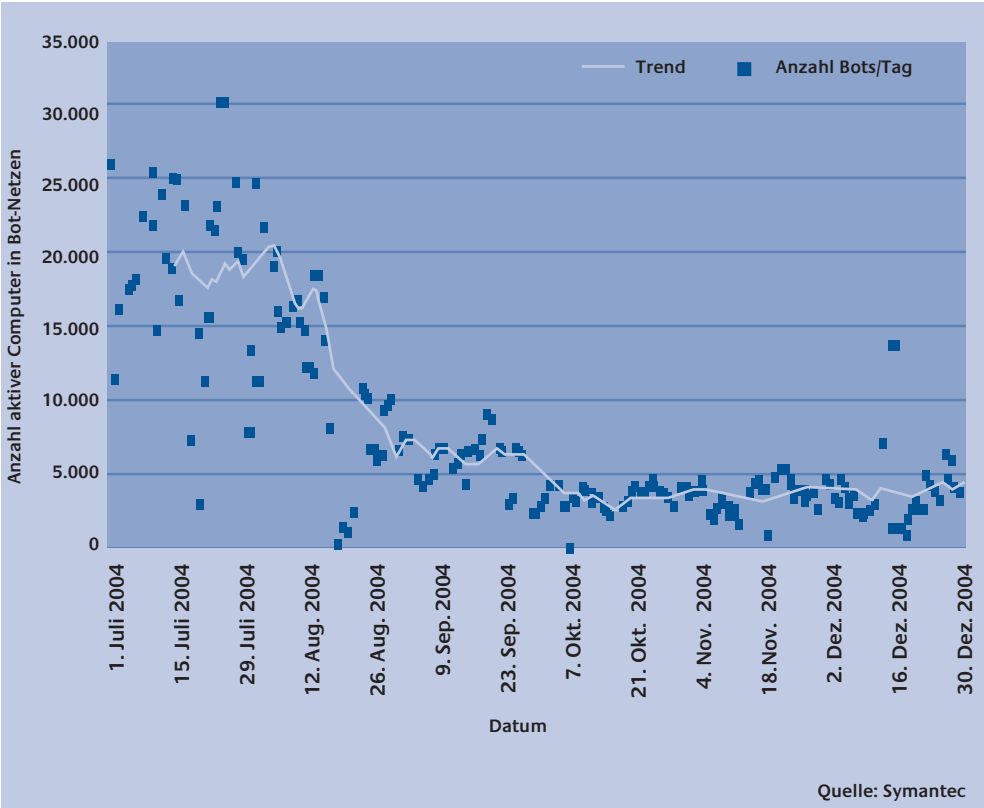

Abbildung 5: Anzahl und Größe von Bot-Netzen weltweit [15]

4.6 Phishing

E-Commerce-Infrastrukturen und Onlinebezahlsysteme sind zunehmend durch Angriffe auf vertrauliche Informationen bedroht. Eine weit verbreitete Methode für Betrugsversuche sind gefälschte E-Mails, so genannte Phishing-Mails. Diese massenhaft versendeten Nachrichten werden mit einer gefälschten Absenderadresse versehen. Die Versender kopieren die Aufmachung offizieller E-Mails bekannter Unternehmen, um das Vertrauen der Kunden zu erschleichen. Über einen Link in der E-Mail werden die Kunden auf eine Webseite geführt, die der Seite des Unternehmens nachempfunden ist. Hier versuchen die Betrüger Nutzerdaten

auszuspähen und an Passwörter, Daten für das Onlinebanking und Kreditkartennummern der Kunden zu gelangen. Diese Informationen werden anschließend für Finanztransaktionen missbraucht.

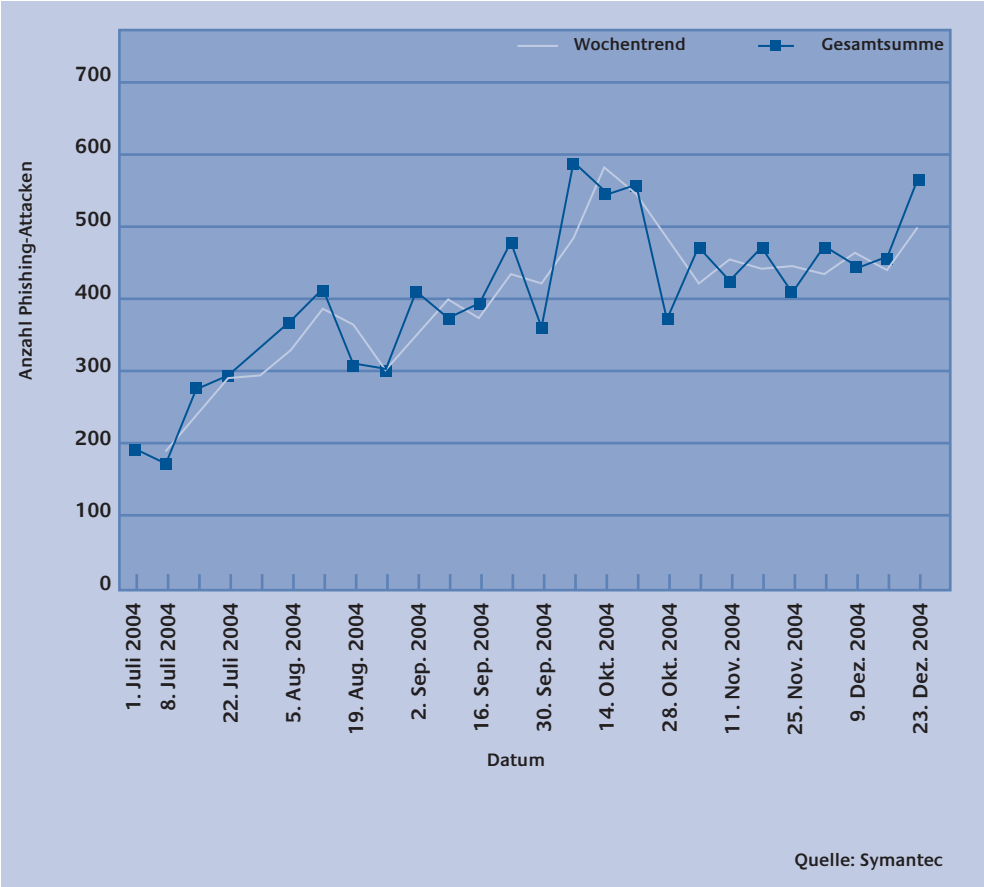

Abbildung 6: Anzahl von Phishing-Mails weltweit [15]

Die Zahl der Phishing-Mails steigt kontinuierlich. Die Methode ist erfolgreich, weil die Anzeige von URL-Adressen im Internetbrowser leicht zu manipulieren ist und noch zu wenige Nutzer auf „Echtheitsmerkmale“ wie Seitenzertifikat und die Verschlüsselung von Webseiten achten. Gleichzeitig werden die Betrugsmethoden immer perfider. Bei einigen Nachrichten öffnen sich zwar im Hintergrund die echten Seiten einer Onlinebank, das im Vordergrund erscheinende Fenster, in das der Kunde seine Daten eintragen soll, stammt jedoch von einem Phishing-Server. In den USA sind darüber hinaus auch Phishing-E-Mails aufgetaucht, in denen

Bankkunden persönlich mit ihrem Namen und ihrer Kontonummer angesprochen werden. Diese Methode kann besonders vertrauenswürdig wirken.

4.7 Dialer

Dialer sind Programme zur Abrechnung einer erbrachten Leistung über die Telefonrechnung (Micro-Payment). Im Internet werden damit kostenpflichtige Informationen oder Downloads abgerechnet. Dazu muss der Betreiber eines Dialers eine Zulassung bei der Regulierungsbehörde für Telekommunikation und Post (Reg TP) beantragen.

Es existieren jedoch auch illegale Dialer, die sich unbemerkt auf dem betroffenen Computer installieren und über teure Rufnummern eine Internetverbindung herstellen, ohne dass der Benutzer dies bemerkt. Oft gehen diese Internetverbindungen ins Ausland oder es werden teure Satellitenverbindungen hergestellt. 2004 war ein merklicher Anstieg dieser illegalen Dialer zu verzeichnen.

4.8 Neue Technologien und IT-Sicherheit

Die Bedeutung neuer Übertragungstechnologien wie Bluetooth, WLAN oder UMTS nimmt zu. Die Zukunft mobiler Anwendungen, die auf drahtlose Kommunikationssysteme aufsetzen, hängt entscheidend von der Bewältigung bestehender Sicherheitsprobleme ab. Ohne Sicherheitsmechanismen können Angreifer leicht Datenverkehr verfolgen, verändern oder anderweitig manipulieren. Im Folgenden wird das Risikopotenzial der wesentlichen neuen Technologien und Anwendungen dargestellt.

4.8.1 Internettelefonie – VoIP

Mit Voice over IP (VoIP) ist Sprachkommunikation nicht mehr auf das Telefonnetz begrenzt, sondern kann auch über IP-basierte Netze wie das Internet übertragen werden. Ein mit dem Internet verbundener Computer übernimmt hier die Funktion des Telefons. Experten gehen davon aus, dass VoIP in den nächsten zehn Jahren die bisherige Telefontechnik vollständig ablösen wird.

Das Internet bietet allerdings hierfür keine besonderen Sicherheitsmechanismen, sodass ein großes Bedrohungspotenzial für neuartige VoIP-Anwendungen besteht. Unverschlüsselte Telefonate lassen sich leichter als im herkömmlichen Telefonnetz abhören, auch sind Angriffe durch massenhaften Spamversand oder die Verbreitung spezieller Schadprogramme zu erwarten.

4.8.2 Mobile Datenübertragung – WLAN

Wireless Local Area Networks (WLAN) werden als ergänzende breitbandige Zugangstechnologie immer stärker genutzt. Bereits 11 Prozent der befragten Unternehmen in Deutschland setzten im Jahr 2004 drahtlos vernetzte Computer ein, im Vorjahr waren es nur 5 Prozent.

In der Nähe eines WLAN-Zugangspunkts, des so genannten „Hotspots“, können mobile Computer wie Notebooks oder PDAs ohne Kabelverbindung Zugriff auf das Internet erhalten. Neben dem Internetzugriff über Hotspots ist die Verwendung von WLAN zur Erweiterung eines kabelgebundenen LANs ein wichtiges Einsatzfeld. Ein nicht ausreichend gesichertes WLAN birgt jedoch große Sicherheitsrisiken. Über einen offenen Zugang kann ein Angreifer beispielsweise sensible Daten sammeln oder unbemerkt modifizieren. Zudem können Spamversender ungesicherte WLANs nutzen, um Spam-Mails zu versenden. Der Nachweis eines solchen Missbrauchs ist nur schwer möglich, da häufig die Zugriffe nicht protokolliert werden. In Zukunft könnten Schadprogramme unmittelbar über drahtlose Netze verbreitet werden. Zudem besteht die Möglichkeit von Imageschäden oder finanziellen Schäden, wenn z. B. strafrechtlich relevante Inhalte heruntergeladen werden.

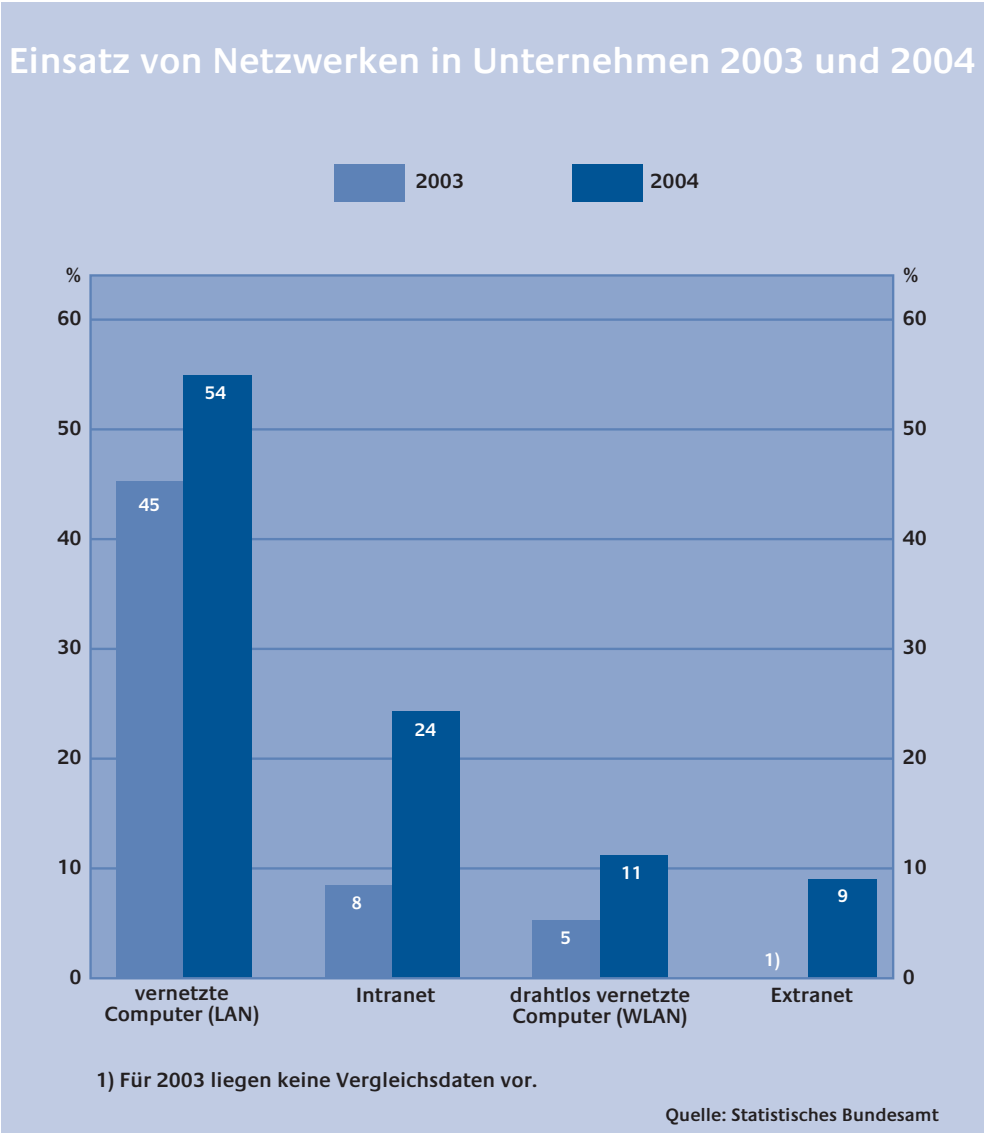

Abbildung 7: Verbreitung von WLANs in deutschen Unternehmen [13]

Die Sicherung von WLANs ist aus verschiedenen Gründen oft ungenügend. Auf Anwenderseite sind die getroffenen Sicherheitsmaßnahmen wie z. B. Zugriffsschutz, Benutzerauthentisierung, restriktive Datei- und Ressourcenfreigabe auf Betriebssystemebene, lokale Verschlüsselung sowie Verwendung nichttrivialer Passwörter oft ungenügend. Auf Herstellerseite ist das in vielen WLAN-Komponenten verwendete Verschlüsselungssystem WEP problematisch. WEP genügt den Sicherheitsansprüchen seit längerem nicht mehr, da der Schutz mit aktuellen Hackerwerkzeugen in relativ

kurzer Zeit aufgehoben werden kann. Bei den auf dem Markt angebotenen WLAN-Adaptern werden jedoch bislang nur selten die sicheren Nachfolgestandards WPA und WPA2 (auch bekannt als IEEE 802.11i) zum Schutz der Funkverbindung verwendet.

4.8.3 Prozessleitsysteme – SCADA

Unternehmen, Verwaltungen und private Haushalte sind von der ständigen Verfügbarkeit von Infrastrukturen beispielsweise zur Strom- oder Wasserversorgung abhängig. Viele dieser Infrastrukturen verwenden spezielle Prozessleitsysteme, auch SCADA-Systeme (Supervisory Control and Data Acquisition) genannt, zur Steuerung der verschiedenen Funktionen. Zur Vernetzung ihrer Komponenten nutzen diese Systeme heute immer häufiger die gleiche Technologie wie Computernetze. Hat ein Angreifer Zugang zum Netz des Prozessleitsystems, kann er von „normalen“ Computersystemen her bekannte Angriffsmethoden nutzen, um die Funktionen des Systems zu beeinträchtigen.

Das Gefahrenpotenzial ist groß, da bei vielen SCADA-Systemen aufgrund der besonderen Anforderungen die Standardsicherheitsmaßnahmen nicht immer angewandt werden. Schutzmaßnahmen wie Netzwerkmonitore, Intrusion-Detection-Systeme und der Einsatz von Firewalls mit sehr restriktiven Regeln dürfen die Funktionalität der Prozessleitsysteme nicht beeinträchtigen.

Bei der Entwicklung vieler SCADA-Komponenten ist der Aspekt der IT-Sicherheit nicht ausreichend berücksichtigt worden. Zudem wurden Sicherheitsmechanismen wie Authentifizierung und Verschlüsselung nicht implementiert. Erschwerend kommt hinzu, dass die Unternehmen für die eingesetzten Prozessleitsysteme zu wenig Risikoanalysen durchführen.

4.8.4 Mobiltelefone und PDAs

Im Jahr 2004 besaß in 78 Prozent der deutschen Haushalte mindestens eine Person ein Mobiltelefon. Deutlich zugelegt hat die Ausstattung mit internetfähigen Mobiltelefonen: 2003 war in 17 Prozent der Haushalte ein solches Mobiltelefon vorhanden, 2004 lag der Wert bereits bei 22 Prozent. 14 Prozent der Haushalte,

die ein internetfähiges Mobiltelefon besitzen, gaben an, das Mobiltelefon auch tatsächlich als Internetzugang zu verwenden [13].

Die Entwicklung moderner Mobiltelefone hin zu kleinen Computern mit eigenem Betriebssystem sowie einer Vielzahl von Anwendungen und Außenschnittstellen birgt eine Reihe von Risiken. Im Juni 2004 trat mit Cabir das erste Schadprogramm für Mobiltelefone auf. Der Wurm ist nur ein „Proof of Concept", also ein Testwurm, und enthält keine Schadfunktion. Er versucht, per Bluetooth Kontakt zu anderen Endgeräten aufzunehmen und sich dort zu installieren.

Das Schadprogramm Dampig A verbreitet sich seit Ende 2004 ebenfalls über Bluetooth und versucht, Cabir-Varianten auf dem Mobiltelefon zu installieren. Neu an diesem Wurm: Er zerstört die Deinstallationsinformationen im System und kann deshalb nur mit einem Antivirenwerkzeug entfernt werden. Ende 2004 gab es ca. 21 bekannte Schadprogramme für mobile Anwendungen, einige bereits in mehreren Varianten.

Derzeit ist das Risiko einer Infektion mobiler Endgeräte durch Schadprogramme noch gering. Bislang sind nur wenige Viren im Umlauf, zudem begrenzt der Übertragungsweg Bluetooth ihre Reichweite auf nur wenige Meter. Allerdings können auch andere Funkschnittstellen wie z. B. GSM oder UMTS für die Verbreitung von Schadprogrammen genutzt werden. In diesem Fall wäre eine Übertragung über größere Distanzen hinweg möglich.

Mit wachsendem Funktionsumfang der mobilen Kommunikationsgeräte nehmen generell die Angriffsmöglichkeiten zu. In Zukunft könnten Daten zerstört und missbraucht oder ungewollt teure Telefonverbindungen aufgebaut werden. Beruflich eingesetzte mobile Endgeräte befinden sich zudem oft außerhalb der Sicherheitsgrenzen des Unternehmensnetzes. Verfügen sie über einen Netzzugang, können sie für einen Einbruch in die IT-Systeme eines Unternehmens missbraucht werden. Schutzmaßnahmen wie Virenscanner oder Firewalls werden zwar mittlerweile auch für eine Reihe mobiler Endgeräte angeboten, sind jedoch noch kaum verbreitet.

4.9 Innentäter, Irrtum und Nachlässigkeit

IT-Schäden innerhalb von Organisationen sind in vielen Fällen auf Innentäter, d. h. eigene Mitarbeiter, zurückzuführen [5]. Da dieser Personenkreis häufig berechtigt ist, auf von außen nicht zugängliche IT-Systeme zuzugreifen, und gleichzeitig über detailliertes internes Wissen verfügt, sind die Auswirkungen unbeabsichtigter Fehlbedienungen oder vorsätzlicher Manipulationen gravierend.

Vorsätzliche Handlungen führen zwar seltener als Irrtum und Nachlässigkeit zu Schäden, ihre Auswirkungen sind dafür kritischer und vor allem schwieriger zu entdecken. Als Motivation der Täter kommen Neugier, Rachegefühle, Neid und persönliche Bereicherung in Frage. Innentäter manipulieren interne Daten zum Nachteil der Organisation oder gelangen an vertrauliche Informationen zu Mitarbeitern, Entwicklungsvorhaben oder Vertragsverhandlungen.

Auch das nachlässige Öffnen von E-Mail-Anhängen mit Schadprogrammen oder das versehentliche Löschen wichtiger Dateien richtet großen Schaden an.

4.10 Strukturelle Schwächen

Die Verlässlichkeit von IT-Strukturen genügt heute immer öfter nicht mehr den gestellten Anforderungen. Ursache ist zum einen der immer komplexere Aufbau einzelner IT-Systeme, deren Zusammenspiel im Gesamtsystem eines Unternehmens oder einer Verwaltung immer schwerer zu durchblicken ist. Hinzu kommen die hohen Innovationsraten in der Informationstechnik und die unzureichenden Ressourcen der IT-Abteilungen in Wirtschaft und Verwaltung.

Beobachtungen des BSI zeigen, dass wesentliche IT-Störungen in Kritischen Infrastrukturen heute häufig nicht auf externe oder interne Angriffe zurückzuführen sind. Bereits ein einfaches Systemversagen zeitigt schwerwiegende Folgen. Aufgrund der umfassenden Vernetzung mit anderen Systemen ziehen Störungen Dominoeffekte nach sich, die zuvor nicht hinreichend bedacht worden sind. Große Probleme ergeben sich aus fehlenden Prozessanalysen, geringen Redundanzen bei IT-Systemen und Leitungsführungen, ungenügenden Krisen- und Notfallplänen sowie einer nicht ausreichenden Sensibilisierung des Managements.

Trends und Entwicklungen bei IT-Bedrohungen

5 Trends und Entwicklungen bei IT-Bedrohungen

Neben Schädigungen durch Computerviren und -würmer erfolgen auch immer wieder zielgerichtete Angriffe auf IT-Systeme durch Hacker. Einige Angriffsmethoden wurden in den vorhergehenden Abschnitten beschrieben. Der folgende Teil beschreibt die Trends bei IT-Angriffen und den Wandel in der Motivation der Angreifer.

5.1 Wirtschaftsspionage

Das Internet eröffnet der Wirtschafts- und Konkurrenzspionage neue Dimensionen. Dabei werden die Methoden zum Ausspähen und Manipulieren von Daten und Diensten immer professioneller. Klassische Ziele sind Technologie- und Know-how-Diebstahl sowie die Erlangung von Wettbewerbsvorteilen etwa durch das Ausspionieren von Ausschreibungen, Verträgen und Preisinformationen. Das Ausspähen von Unternehmensnetzen mit dem Ziel der unbefugten Kenntnisnahme von Unternehmensdaten wird in den nächsten zehn Jahren an Bedeutung zunehmen [4].

Innentäter, also z. B. Angestellte eines Unternehmens oder externe Berater, stellen in diesem Kontext ein besonderes Sicherheitsproblem dar. Während beispielsweise Hacker zunächst noch versuchen müssen, von außen die IT-Sicherheitssysteme eines Unternehmens zu überwinden, befindet sich der Innentäter schon innerhalb dieser Systeme. Auch der anhaltende Trend zum Outsourcing von Dienstleistungen ist problematisch. Hier können externe Personen Zugang zu sensiblen Daten oder Einblick in interne Sicherheitsstrukturen erhalten.

Der Verlust der Vertraulichkeit von Daten kann wirtschaftlichen Schaden für das betroffene Unternehmen zur Folge haben. Konkurrenten könnten Einsicht in sensible Dokumente zur Forschung und Entwicklung von Produkten oder in Angebote erhalten. Unter dem Bekanntwerden eines Datenmissbrauchs leidet nicht zuletzt auch das Image des Unternehmens.

Gefährdet von Wirtschafts- und Konkurrenzspionage sind nahezu alle Unternehmensbereiche, wobei Forschungs- und Entwicklungsabteilungen am stärksten bedroht sind. Unternehmen mit großen, werthaltigen Entwicklungsbereichen wie beispielsweise Pharmaunternehmen, Unternehmen der Automobilindustrie sowie Softwarefirmen sind besonders gefährdet [6]. Dem Schutz von geistigem Eigentum wird in vielen Bereichen kein ausreichender Stellenwert zugewiesen, was daran liegt, dass auf Managementebene das Bewusstsein für IT-gestützte Wirtschaftsspionage nicht ausreichend ausgeprägt ist.

5.2 Gegen Infrastrukturen gerichtete Angriffe

Künftig werden nicht mehr nur einzelne Computer das Ziel von Hackern sein. Es ist beispielsweise mit einem rapiden Anstieg von Angriffen auf die Namensserver (DNS) zu rechnen, die für die Zuordnung eines Hostnamens zu einer IP-Adresse zuständig sind. Die Internetnutzer können durch diese manipulierten Server massenhaft auf gefälschte Phishing-Webseiten fehlgeleitet werden.

Zunehmend stehen auch Router, Firewalls und andere Sicherheitseinrichtungen, die in Unternehmen oder Verwaltungen Systeme schützen sollen, im Fokus der Angreifer. Solche Angriffe sind von einer neuen Qualität, da ganze Rechnernetze betroffen sind. Angriffe auf Router können dazu führen, dass das angeschlossene Netz seine Verbindungen zum Internet verliert.

Nicht zuletzt durch die zunehmende IT-Durchdringung aller Lebensbereiche stellt der Schutz der in Abschnitt 4.8.3 beschriebenen Prozessleitsysteme eine wichtige Herausforderung dar. Bei Produktentwicklungen in diesem Bereich hat IT-Sicherheit bislang nur eine untergeordnete Rolle gespielt.

5.3 Gezielte Angriffe gegen Unternehmen

Angriffe auf IT-Systeme hatten schon 2004 einen vorwiegend wirtschaftlichen Hintergrund. 16 Prozent der Hackeraktivitäten zielten auf E-Commerce-Unternehmen, was im Vergleich zum Vorjahr einem Zuwachs um 400 Prozent entspricht [14]. Ziel war vor allem das Ausspionieren von Kreditkarteninformationen und anderen sensitiven Finanzdaten. Für die Zukunft wird befürchtet, dass sich dieser Trend weiter verstärkt.

Ein großes Sicherheitsproblem stellen auch gezielte DDoS-Angriffe gegen Unternehmen dar. Lanciert von der Konkurrenz, unzufriedenen Mitarbeitern oder von anders motivierten Personenkreisen, beeinträchtigen solche Angriffe die Funktionsfähigkeit von Servern massiv. Gerade für E-Commerce-Unternehmen kann dies erhebliche wirtschaftliche Folgen haben.

5.4 Kriminalisierung und Fokus auf finanziellen Gewinn

Wurde Angriffen auf IT-Systeme bisher häufig „sportlicher Ehrgeiz“ unterstellt, verliert dieser Aspekt zunehmend an Bedeutung [6]. Es zeichnet sich ein Trend hin zur Professionalisierung und Kommerzialisierung der Internetkriminalität ab. Statt isolierter Computerhacker steht hinter gerichteten Angriffen vermehrt die organisierte Kriminalität. Hacker und Virenautoren arbeiten mit den Kriminellen zusammen und schreiben Schadprogramme für Phishing, Kreditkartenbetrug und Erpressungstricks.

Finanzielle Interessen sind dabei die ausschlaggebende Antriebskraft. Durch den Missbrauch von IT-Systemen lässt sich mittels der Verbreitung von Spam sowie des Missbrauchs sensibler Daten wie Kreditkartennummern oder Onlinebankingdaten Geld verdienen.

Die von einer zunehmenden Kriminalisierung der Angriffe ausgehende veränderte Bedrohungslage ist in ihrer Ausprägung bislang nur schwer zu bewerten. Aufgrund des finanziellen Anreizes erwartet das BSI, dass die zunehmende Kriminalisierung auch im kommenden Jahr ein ernstes Problem darstellen wird.

5.5 Regionalisierung von Schadprogrammen

Verwendeten Programmierer von Schadsoftware bislang vor allem englischsprachige E-Mails, um Computerwürmer zu verbreiten, so sind inzwischen vermehrt deutschsprachige Texte zu registrieren. Diese Regionalisierung führt zu einer weiten Verbreitung solcher Schadprogramme in Deutschland.

Im Mai 2005 verbreitete sich beispielsweise eine Variante des Computerwurms Sober in E-Mails im Zusammenhang mit der laufenden Ticketvergabe für die Fußball-WM in Deutschland 2006. Die Versender täuschten die Benachrichtigung über einen Ticketverkauf vor.

Aktivitäten

6 Aktivitäten

Dieser Lagebericht gibt einen Überblick zum Status quo sowie den sich abzeichnenden Entwicklungen der IT-Bedrohungen in Deutschland. Aus der Analyse der gegenwärtigen Lage entsteht Handlungsbedarf. In den folgenden Abschnitten werden erforderliche Maßnahmen sowie Aktivitäten der für IT-Sicherheit zuständigen Bundesbehörden dargestellt.

6.1 Bürgerinnen und Bürger

Im Bereich IT-Sicherheit trägt jeder einzelne Computernutzer eine Mitverantwortung im Kampf gegen Hackerangriffe sowie die Verbreitung von Schadprogrammen und Spam. Angesichts der beschriebenen Bedrohungen müssen nicht nur Wirtschaft und Verwaltung, sondern gerade auch Bürgerinnen und Bürger Sorge dafür tragen, dass die im Haushalt verwendeten IT-Systeme sicher sind. Durch Aufklärungsangebote wie die Internetseite www.bsi-fuer-buerger.de kann sich jeder IT-Nutzer über aktuelle Sicherheitsthemen informieren.

Mit dem **Internetportal www.bsi-fuer-buerger.de** wendet sich das BSI speziell an private Internetnutzer. Hier finden auch Menschen ohne IT-Vorwissen allgemein verständlich formuliert wichtige Informationen rund um das Thema IT-Sicherheit. Neben Ratschlägen und Hinweisen gibt es zahlreiche Programme zum kostenlosen Download. Zudem können Internetnutzer den kostenlosen Newsletter „SICHER • INFORMIERT“ abonnieren. Er erscheint alle zwei Wochen, wird per E-Mail zugesandt und enthält aktuelle IT-Sicherheitsinformationen.

6.2 Wirtschaft

Die in diesem Bericht beschriebenen Defizite machen deutlich, dass das Management der Unternehmen, aber auch die Mitarbeiter stärker sensibilisiert werden müssen. Die Vertraulichkeit von Daten in Unternehmen muss gesichert und der Schutz vor gezielten Angriffen verstärkt werden. Um dieses Ziel zu erreichen, sollte in den Unternehmen zunächst eine IT-Strukturanalyse durchgeführt werden; auf dieser Grundlage kann eine Schutzbedarfsfeststellung erfolgen. Die Erkenntnisse fließen dann in eine auf die eigenen Bedürfnisse abgestimmte Sicherheitspolicy ein. Für die Umsetzung der IT-Sicherheitsstrategie bedarf es der notwendigen personellen wie finanziellen Ressourcen. Sicherheitskultur muss zum integralen Bestandteil der Unternehmenskultur werden.

Um auf Vorfälle in Netzen schnell und effizient reagieren zu können, sind auch Krisenmanagementfähigkeiten inklusive Notfallplänen notwendig. Die Wirksamkeit der getroffenen Sicherheitsmaßnahmen wird durch regelmäßige Sicherheitsrevisionen sichergestellt.

Das **Mcert (www.mcert.de)** ist eine Initiative unter der Federführung des Bundesverbands Informationswirtschaft, Telekommunikation und neue Medien e. V. (BITKOM) in Form einer Public-Private-Partnership mit dem Bundesministerium des Innern und dem Bundesministerium für Wirtschaft und Arbeit sowie Partnern aus der Wirtschaft. Mcert ist ein neutrales Kompetenzzentrum für IT-Sicherheit. Die Leistungen sind speziell auf die Bedürfnisse kleiner und mittlerer Unternehmen abgestimmt. Mcert bietet verständliche und verlässliche Sicherheitsinformationen und Handlungsempfehlungen. Dazu gehören etwa speziell zugeschnittene und bewertete Warnmeldungen zu Schadprogrammen oder Hinweise auf aktuelle Sicherheitslücken.

6.3 Verwaltung

Funktionierende IT-Systeme, Datenschutz und Vertraulichkeit sowie Mitarbeiter mit angemessener IT-Sicherheitskompetenz sind aus Sicht der IT-Sicherheit grundlegende Elemente für eine funktionierende Verwaltung. Ein wichtiger Schritt zu sicheren IT-Systemen in der Verwaltung ist die Realisierung eines angemessen hohen Sicherheitsniveaus in allen Behörden. Analog zur Wirtschaft sollten auch in der Verwaltung IT-Sicherheitsmanagementsysteme installiert werden. Hierzu gehört zunächst die Benennung von IT-Sicherheitsbeauftragten, die im Auftrag der Behördenleitung die Erstellung und Umsetzung von IT-Sicherheitskonzepten koordinieren.

Ebenso wie in der Wirtschaft sind in Behörden auch Krisenmanagementfähigkeiten und Notfallpläne notwendig. Auch die Prüfung der Sicherheitsmaßnahmen durch entsprechende Revisionen ist von zentraler Bedeutung.

Das **Computer-Emergency-Response-Team des Bundes (CERT-Bund – www.bsi.bund.de/certbund)** ist bei sicherheitsrelevanten Vorfällen in IT-Systemen der Bundesverwaltung die zentrale Anlaufstelle für präventive und reaktive Maßnahmen. Zu den Aufgaben des CERT-Bund zählen unter anderem der Hinweis auf Schwachstellen in Hardware- und Softwareprodukten, die Warnung und Alarmierung bei besonderen IT-Bedrohungslagen und die Empfehlung von reaktiven Maßnahmen zur Schadensbegrenzung oder -beseitigung. Die Dienstleistungen des CERT-Bund stehen in erster Linie den Bundesbehörden zur Verfügung. Sie umfassen neben einer 24-Stunden-Rufbereitschaft unter anderem einen Warn- und Informationsdienst und die Alarmierung der Bundesverwaltung bei akuten IT-Gefährdungen. Anfragen von anderen Behörden sowie Privatpersonen oder privaten Institutionen werden im Rahmen verfügbarer Ressourcen bearbeitet.

6.4 Nationales IT-Sicherheitskompetenzzentrum

Das Bundesamt für Sicherheit in der Informationstechnik hat den Auftrag, zur Verbesserung der IT-Sicherheit in Deutschland beizutragen. Dazu untersucht das BSI Sicherheitsrisiken bei der Anwendung der Informationstechnik und entwickelt in Einzelfällen entsprechende Sicherheitsvorkehrungen. Es informiert über Risiken und Gefahren beim Einsatz der Informationstechnik und hilft bei der Lösung von konkreten Problemstellungen.

Dies beinhaltet die Prüfung und Bewertung der Sicherheit von IT-Systemen, einschließlich deren Entwicklung in Kooperation mit der Industrie. Um die genannten Risiken zu minimieren oder ganz zu vermeiden, wendet sich das BSI an eine Vielzahl von Zielgruppen, indem es Hersteller, Vertreiber und Anwender von Informationstechnik berät. Darüber hinaus analysiert es Entwicklungen und Trends in der Informationstechnik.

Für die verschiedenen gesellschaftlichen Zielgruppen bietet das BSI spezifische Informations- und Beratungsdienste an. Während das Computer-Emergency-Response-Team der Bundesverwaltung (CERT-Bund) über den Warn- und Informationsdienst umfangreiche Informationen über neue Schwachstellen und Bedrohungen anbietet, informiert das Portal www.bsi-fuer-buerger.de die privaten IT-Nutzer.

Die Zunahme und Veränderung der IT-Bedrohungen erfordert vom BSI neue Denk- und Handlungsweisen. Um die oben beschriebenen Aufgaben weiterhin angemessen wahrnehmen und zudem gegen neue Gefahren effektive Schutzmaßnahmen entwickeln und diese zeitnah umsetzen zu können, arbeitet das BSI eng mit Experten aus anderen Behörden im In- und Ausland, aber auch mit der Wirtschaft zusammen. Neu geschaffene Stellen tragen dazu bei, auch der Bedeutung neuer Aufgaben gerecht zu werden und jederzeit auf breites Expertenwissen zurückgreifen zu können. Mit seinen Kompetenzen unter anderem in den Bereichen Zertifizierung, IT-Grundschutz und Kryptotechnologie schafft das BSI Grundlagen, um auch kommenden Herausforderungen für die IT-Sicherheit in Deutschland effektiv begegnen zu können.

Zukünftig wird das BSI verstärkt operativ tätig. Neben den genannten Aufgaben stellt die IT-Sicherheitsbetreuung der Bundesverwaltung weiterhin den zentralen Bestandteil der Arbeit dar.

Über die **BSI-Homepage www.bsi.bund.de** sind aktuelle Warnhinweise, Onlineangebote und weitere Informationen rund um die Sicherheit in der Informationstechnik jederzeit abrufbar. Zu Kernthemen des BSI wie zum Beispiel IT-Grundschutz, Zertifizierung/Akkreditierung, Internetsicherheit und Schutz Kritischer Infrastrukturen steht ein umfangreiches Onlineangebot zur Verfügung. Zudem sind zahlreiche BSI-Studien zu verschiedenen Fachthemen abrufbar.

6.5 Gemeinschaftliches Handeln

IT-Sicherheit ist gleichermaßen unverzichtbar für die Innere Sicherheit und für die Sicherung des Wirtschaftsstandortes Deutschland. Der Staat ist nicht nur gefordert, Angebote zur Sensibilisierung und Aufklärung über Risiken beim Umgang mit IT zur Verfügung zu stellen. Er sollte darüber hinaus Sorge tragen, dass IT-Sicherheit sowohl auf Bundesebene als auch in den Unternehmen umfassend in alle Prozesse integriert wird.

Entsprechende Maßnahmen setzen auf verschiedenen Ebenen an: Zum einen müssen IT-Systeme möglichst gut gegen bestehende und künftige IT-Bedrohungen abgesichert sein. Da Störungen in komplexen IT-Systemen nie ganz ausgeschlossen werden können, ist darüber hinaus auch eine schnelle Reaktionsfähigkeit über ein nationales IT-Krisenmanagement notwendig. Um den langfristigen Schutz von IT-Systemen zu gewährleisten, muss schließlich die IT-Sicherheitskompetenz in Wissenschaft und Wirtschaft gestärkt werden.

Fazit

7 Fazit

In dem Maße, wie Informationstechnik alle Lebensbereiche erfasst, gefährden gerichtete Angriffe und Schadprogramme zunehmend sowohl private Anwender als auch Wirtschaft und Verwaltung. Der Lagebericht zeigt bereits bestehende und sich entwickelnde Bedrohungen der Informationstechnik auf, mit denen sich alle gesellschaftlichen Gruppen auseinander setzen müssen.

Noch ist die Lage beherrschbar. Damit unsere Informationstechnik aber auch in Zukunft zuverlässig funktioniert, muss das Bewusstsein für die Wichtigkeit von IT-Sicherheit weiter geschärft werden. Auf der Ebene von Unternehmen und Verwaltungen sollten Maßnahmen wie Risikoanalysen, die Erstellung von IT-Sicherheitskonzepten, die Ernennung von IT-Sicherheitsbeauftragten sowie IT-Sicherheitsrevisionen eine Selbstverständlichkeit sein. Aber auch Bürgerinnen und Bürger müssen stärker sensibilisiert und informiert werden, damit auch sie ihre Sicherheitskompetenz erhöhen können.

Nur mit einer neuen, von allen gesellschaftlichen Gruppen in Deutschland getragenen Sicherheitskultur lassen sich die Rahmenbedingungen für sichere und zuverlässige Informationstechnik entscheidend verbessern.

8 Quellen

[1] BSI: Antispam-Strategien. Unerwünschte E-Mails erkennen und abwehren. Köln 2005.

[2] BSI: Bevölkerungsrepräsentative Umfrage des BSI zur IT-Sicherheit in Deutschland. Oktober 2004.

[3] BSI: BSI-Monitoring. Repräsentative Umfrage unter IT-Beauftragten, Datenschutzbeauftragten und Journalisten zur Evaluierung der Öffentlichkeitsarbeit des BSI. Februar 2004.

[4] BSI-Erhebungen.

[5] BSI: IT-Grundschutzhandbuch 2005. Bonn 2005.

[6] BSI: Kommunikations- und Informationstechnik 2010+3: Neue Trends und Entwicklungen in Technologien, Anwendungen und Sicherheit. Bonn 2003.

[7] Capgemini-Studie: IT-Trends 2005. Paradigmenwechsel in Sicht. http://www.de.capgemini.com/servlet/PB/show/1556864/Capgemini_IT_Trends_2005.pdf.

[8] InformationWeek: IT-Security 2004.

[9] kes/Microsoft-Sicherheitsstudie: Lagebericht zur Informations-Sicherheit. http://www.kes.info/archiv/material/studie2004/04-4-006.htm.

[10] McAfee-Studie: Virtual Criminology Report. http://www.mcafeesecurity.com/de/local_content/brochures/studie_virtuelle_kriminalitaet.pdf.

[11] Metagroup: IT-Security im Jahr 2003 (Deutschland). http://www.metagroup.de.

[12] Silicon.de: IT-Security 2004. Im Wettlauf mit der Lernfähigkeit der Hacker. Auszüge aus einer Studie von silicon.de zum Thema IT-Sicherheit. http://www.silicon.de/cpo/downloads/siliconDEStudie_IT-Sicherheit2004.pdf.

[13] Statistisches Bundesamt: Informationstechnologie in Unternehmen und Haushalten 2004.
http://www.destatis.de/download/d/veroe/pb_ikt_04.pdf.

[14] Symantec Internet Security Threat Report, Volume VI (September 2004).
http://enterprisesecurity.symantec.com/content.cfm?articleid=1539.

[15] Symantec Internet Security Threat Report, Volume VII (März 2005).
http://enterprisesecurity.symantec.de/content.cfm?articleid=1591.

9 Glossar

Backdoor
Teil eines Programms, das einen Zugriff auf IT-Systeme vorbei an jeglichen Sicherheitsmechanismen ermöglicht. Diese „Hintertüren“ sind nur zu erkennen, wenn der Quellcode des Programmes offen gelegt ist.

Bot-Netze
In der Fachsprache beschreibt Bot ein Programm, das ferngesteuert arbeitet. Bots können als Verbreitungsweg für Computerviren und -würmer verwendet und von einem Angreifer zentral ferngesteuert werden. Unter Bot-Netz versteht man einen virtuellen Verbund infizierter IT-Systeme, also eine Zusammenschaltung mehrerer Bots bzw. der infizierten Rechner.

Computervirus
Ein Computervirus ist eine nicht selbstständige Programmroutine, die sich selbst reproduziert und dadurch vom Anwender nicht kontrollierbare Manipulationen in Systembereichen, an anderen Programmen oder deren Umgebung vornimmt.

Computerwurm
Ein Computerwurm ist ein selbstständiges, selbstreproduzierendes Programm, das sich in einem System (vor allem in Computernetzwerken) ausbreitet.

DoS-, DDoS-Attacke
Engl. Abk. „Denial of Service“ = außer Betrieb setzen. Angriff auf die Verfügbarkeit der Ressourcen und Dienste eines IT-Systems mit dem Ziel, diese zu blockieren und somit regulären Benutzern keinen Zugriff mehr zu ermöglichen. DDoS: Der zur Blockade führende Angriff wird nicht nur von einem einzelnen Rechner ausgeführt, sondern von mehreren gleichzeitig. Dadurch wird sowohl der Angriff verstärkt als auch die Einleitung der Gegenmaßnahmen erschwert, da diese auf mehrere Quellen angewendet werden müssen.

Gerichteter Angriff
Unter gerichteten Angriffen sind bösartige Versuche zu verstehen, die Schutzziele und die jeweiligen Sicherheitsrichtlinien eines bestimmten Systems durch Ausnutzen von Schwachstellen in Betriebssystem oder Programmen verletzen. Siehe auch DoS-, DDoS-Attacke.

IVBB
Der Informationsverbund Berlin-Bonn (IVBB) stellt die Infrastruktur für die interne Kommunikation der Bundesbehörden dar. Über den IVBB werden die elektronischen Informations-, Kommunikations- und Transaktionsdienstleistungen realisiert.

Patch
Engl. „Flicken"; kleines Programm, das Softwarefehler wie z. B. Sicherheitslücken in Anwendungsprogrammen oder Betriebssystemen behebt.

Phishing
Kunstwort, das sich aus „password" und „fishing" zusammensetzt. Es bezeichnet eine Methode, um mithilfe gefälschter E-Mails an vertrauliche Daten zu gelangen.

Spam
Unerwünschte Nachrichten und „Wurfsendungen" in elektronischer Form (E-Mail). Oft sind sie kommerzieller Art und werden an viele nicht daran interessierte Empfänger gesendet.

Trojanisches Pferd
Trojanische Pferde (auch: Trojaner) sind Programme, die neben scheinbar nützlichen auch nicht dokumentierte schädliche Funktionen enthalten und diese unabhängig vom Computeranwender und ohne dessen Wissen ausführen. Im Gegensatz zu Computerviren können sich Trojanische Pferde jedoch nicht selbstständig verbreiten.

VoIP
Unter VoIP (Voice over Internet Protocol) versteht man das Telefonieren über das Internet. Die Sprachdaten werden dabei in digitale Form umgewandelt, in kleinen Datenpaketen über das Internet verschickt und beim Empfänger wieder zusammengesetzt.

Herausgeber
Bundesamt für Sicherheit
in der Informationstechnik – BSI
53175 Bonn

Bezugsstelle
Bundesamt für Sicherheit
in der Informationstechnik – BSI
Referat III 2.1 (Öffentlichkeitsarbeit)
Godesberger Allee 185–189, 53175 Bonn
Tel: +49-228-95 82-0, E-Mail: bsi@bsi.bund.de
Internet: www.bsi.bund.de

Texte und Redaktion
Referat III 2.1 (Öffentlichkeitsarbeit)
Zucker.Kommunikation, Berlin

Layout und Gestaltung
Zucker.Kommunikation, Berlin
Internet: www.zucker-kommunikation.de

Druck
Pinguin Druck, Berlin

Stand
Juli 2005