



Bundesamt
für Sicherheit in der
Informationstechnik

Die Lage der IT-Sicherheit in Deutschland 2009

Inhaltsverzeichnis

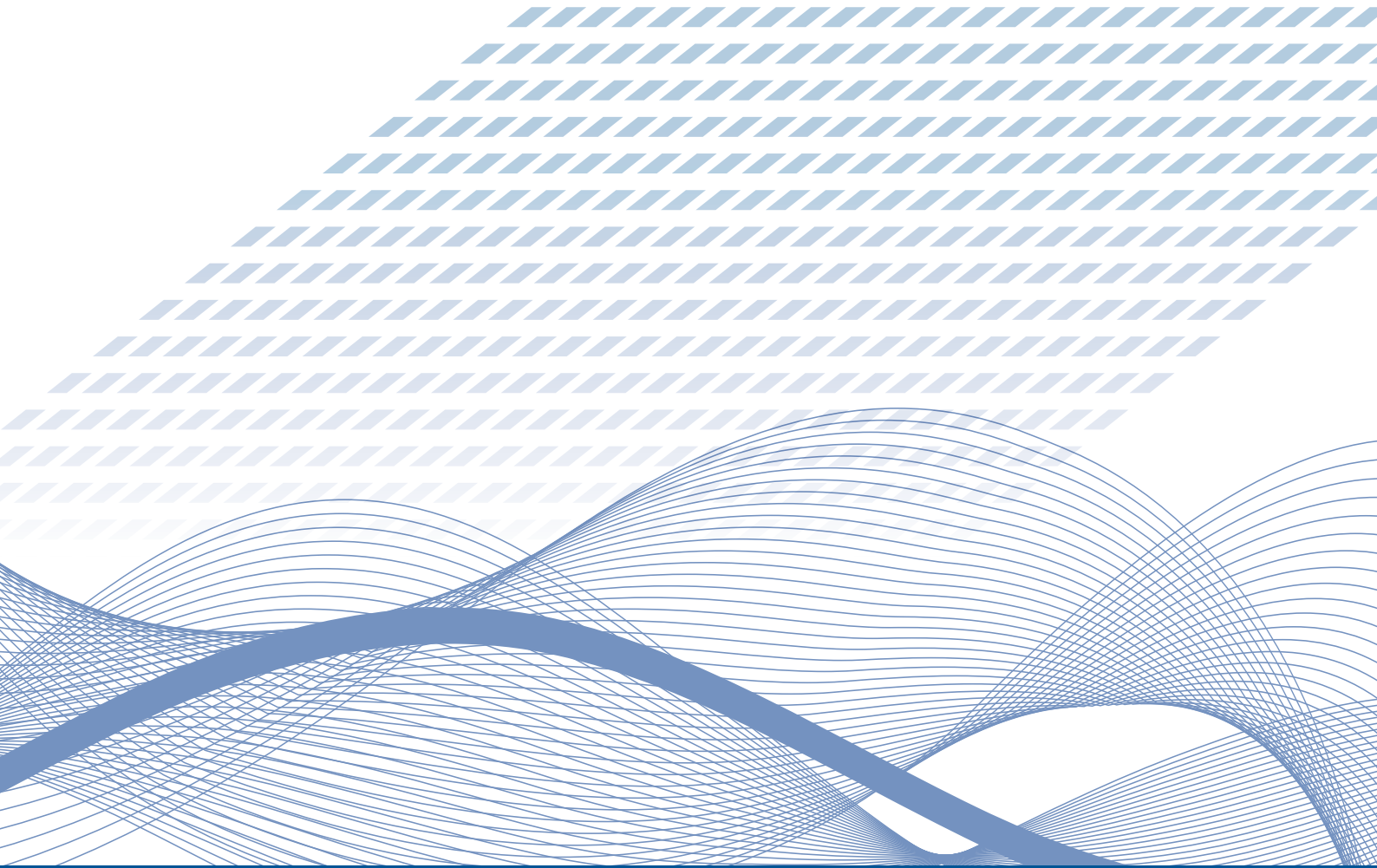
1	Vorwort	5
2	Einleitung	7
3	IT-Sicherheitsbewusstsein und IT-Sicherheitskompetenz in der Gesellschaft	11
3.1	Bürger	11
3.2	Wirtschaft	13
3.3	Verwaltung	16
4	Schwachstellen und Bedrohungen von IT-Systemen	19
4.1	Sicherheitslücken	19
4.2	Schadprogramme	20
4.2.1	Trojanische Pferde	22
4.2.2	Spyware	22
4.3	DoS-Angriffe	23
4.4	Unerwünschte E-Mails (Spam)	24
4.5	Bot-Netze	26
4.6	Identitätsdiebstahl	28
4.7	Betrügerische Webangebote	29
4.8	Kompromittierende Abstrahlung	30
4.9	Materielle Sicherheit, Innentäter, Irrtum und Nachlässigkeit	30
5	Angriffsmöglichkeiten und IT-Sicherheit in ausgewählten Anwendungen und Technologien	33
5.1	Voice over IP (VoIP)	33
5.2	Mobile Kommunikation	34
5.3	Web 2.0	37

5.4	Prozesssteuerungssysteme - SCADA	39
5.5	Internetdienst: Domain Name System (DNS)	40
5.6	Multifunktionsgeräte	41
5.7	Schnittstellen und Speichermedien	42
5.8	Netzkoppelemente	43
5.9	Service-orientierte Architekturen (SOA)	44
6	Chancen und Risiken innovativer Anwendungen und Technologien	47
6.1	Radio Frequency Identification (RFID)	47
6.2	Biometrie, Personaldokumente und Bürgerservices	48
6.3	IPv6	50
6.4	IT-Sicherheit in Automobil und Verkehr	51
6.5	Elektronische Gesundheitskarte (eGK)	52
7	Trends	55
7.1	Wirtschaftliche und gesellschaftliche Trends	55
7.2	Technik-Trends	57
7.3	Rechtliche Trends	60
8	Aktivitäten	63
8.1	Bürger	63
8.2	Wirtschaft	64
8.3	Verwaltung	66
8.4	Zukunftsfonds	67
9	Fazit	69
10	Quellen	74
11	Glossar	76

Abbildungsverzeichnis

Abb.1:	Thematische Schwerpunkte der Internetnutzung in Deutschland	12
Abb.2:	Gründe für Sicherheitsinvestitionen in deutschen Unternehmen	14
Abb.3:	Einschätzung des Sicherheitsrisikos in deutschen Unternehmen	15
Abb.4:	Prozentualer Anstieg des Spam-Aufkommens in der Bundesverwaltung	24
Abb.5:	Anzahl der auf Informationsdiebstahl spezialisierten Command-and-Control-Server 2007 und 2008	27
Abb.6:	Einsatz und geplante Einführung von Voice over IP in deutschen Unternehmen	33
Abb.7:	Teilnehmerentwicklung und Penetration in deutschen Mobilfunknetzen	34
Abb.8:	Einsatz von Wireless LAN (WLAN) in deutschen Unternehmen	36
Abb.9:	Wahrscheinlichkeiten für das Vorhandensein bestimmter Schwachstellen	38
Abb.10:	Absicherung von Peripherie-Schnittstellen (zum Beispiel USB) in deutschen Unternehmen	43
Abb.11:	Entwicklung von IT-Bedrohungen nach Einschätzung des BSI	69
Abb.12:	Risikopotenzial für Angriffsmöglichkeiten in ausgewählten Anwendungen und Technologien nach BSI-Einschätzung [6]	70
Abb.13:	Risikoprofil innovativer Anwendungen und Technologien nach Einschätzung des BSI	70

Vorwort



1 Vorwort

Bereits zum dritten Mal veröffentlicht das BSI den Lagebericht zur IT-Sicherheit in Deutschland. Von einer Entspannung der Situation kann derzeit immer noch keine Rede sein.

Es gibt verschiedene Motivationen, IT-Systeme anzugreifen. Finanzielle Bereicherung zählt zu den Hauptgründen. Durch die zunehmende Verlagerung alltäglicher Aktivitäten – wie Bankgeschäfte tätigen oder Einkaufen – ins World Wide Web ist IT-Kriminalität für die Angreifer ein lohnenswertes Geschäft bei vergleichsweise niedrigem Risiko. So wundert es nicht, dass die Professionalisierung der Internetkriminalität weiter fortschreitet.

Aus der Psychologie wissen wir, dass eine erfolgreiche Sensibilisierung für ein Thema von fortlaufenden Aktionen abhängig ist – die Reaktionsstärke steigt bei Gefahren und lässt schließlich wieder nach. Bedingt durch den Anstieg konkreter Schadensfälle hat das Thema IT-Sicherheit einen höheren Stellenwert auf der Agenda von Staat, Wirtschaft und auch von Privatanwendern eingenommen. Erfreulicherweise ist gegenwärtig auch bei Herstellern und Providern ein Vorstoß zur Verbesserung der Sicherheitseigenschaften von Produkten zu verzeichnen.

Dennoch – dauerhafte Erfolge sind nicht von heute auf morgen zu realisieren. Die ständige Weiterentwicklung von IT-Systemen und immer ausgefeiltere Angriffsmethoden erschweren die Bekämpfung und Verhinderung von Internetkriminalität.

Mit seinen mehr als 500 Mitarbeitern und Partnerschaften auf nationaler und internationaler Ebene arbeitet das BSI kontinuierlich an der Verbesserung des IT-Sicherheitsniveaus in der Bundesrepublik. Eine von allen gesellschaftlichen Gruppen getragene, fest etablierte Sicherheitskultur steckt bezüglich ihres Entwicklungsprozesses zwar noch in den sprichwörtlichen Kinderschuhen, der richtige Weg ist aber bereits eingeschlagen.

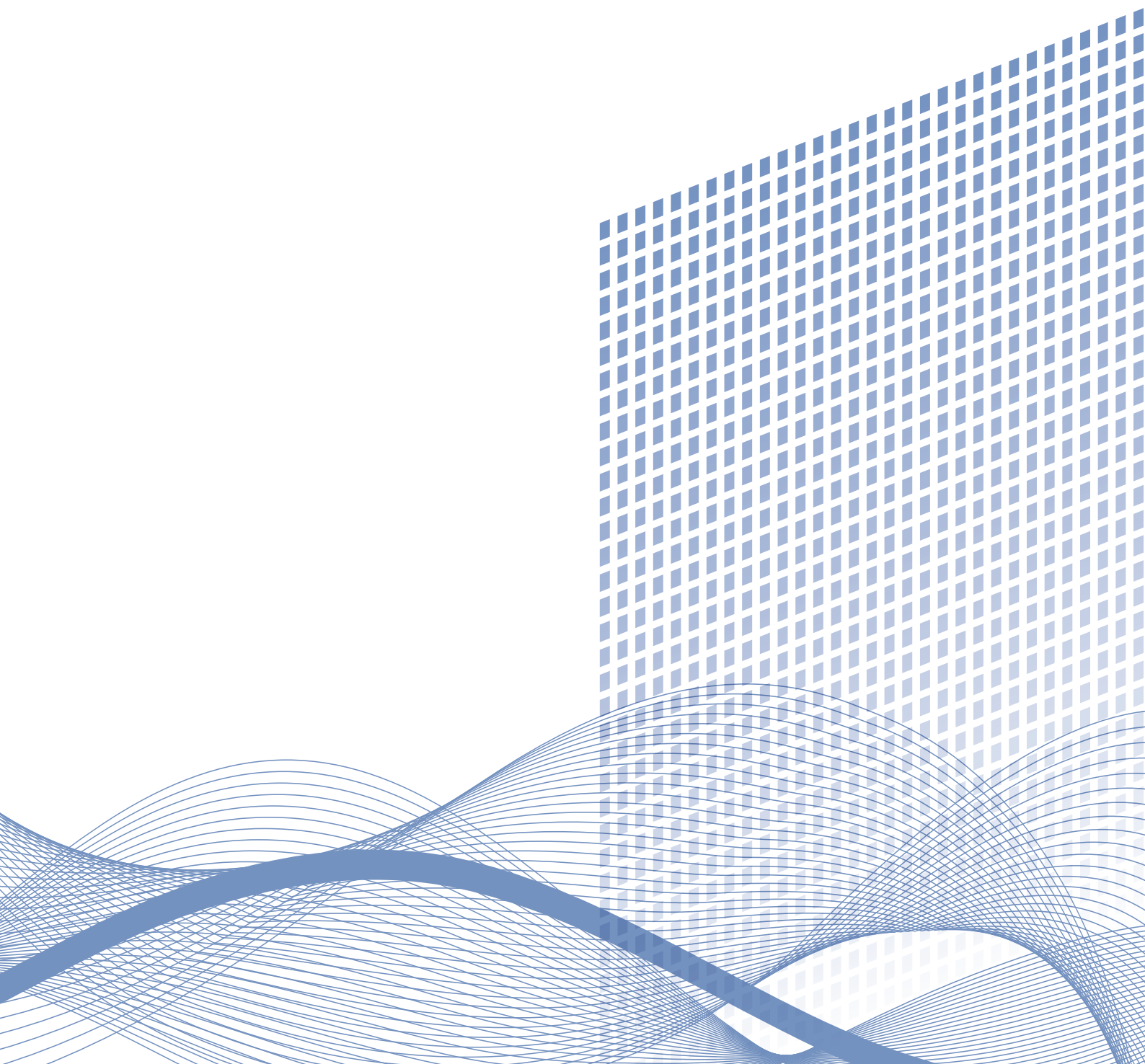
Januar 2009



Dr. Udo Helmbrecht

Präsident des BSI

Einleitung



2 Einleitung


Die Dynamik im Bereich der Informationstechnik ist ungebrochen hoch. Nutzer in Unternehmen, Behörden, aber auch im privaten Bereich sehen sich permanent mit neuen Anwendungen und somit auch mit neuen Bedrohungen konfrontiert.

Die fortschreitende Allgegenwärtigkeit von Informationstechnik sowie deren Miniaturisierung verstärken diesen Trend. Über die unterschiedlichsten Geräte wird heute von unterwegs mit Geschäftspartnern oder dem eigenen Unternehmen kommuniziert. Die Informationen und Dienste der digitalen Welt werden mobil und sind an jedem beliebigen Ort abrufbar. Die permanente Nutzung, Erzeugung, Verarbeitung, Übertragung und Speicherung von Informationen ist längst kein Trend mehr, sondern aus vielen Bereichen nicht mehr wegzudenken. Intelligente Systeme und Gegenstände beherrschen den Alltag.

Immer häufiger wird in den Medien auch über kriminelle Angriffe auf Daten von Unternehmen, Behörden und Privatnutzern berichtet. Datenschutz-Skandale sorgten in der jüngeren Vergangenheit für Aufsehen. Der Umgang mit Daten innerhalb vieler Unternehmen ist problematisch. Oft fehlen personelle und finanzielle Ressourcen sowie technisches Know-how. Technische Schutzmaßnahmen zur Datensicherung sind jedoch besonders wichtig, da Angriffe durch neue und komplexe Techniken zunehmend schwerer zu bekämpfen sind. Aber auch die innovativsten technischen Sicherheitsmaßnahmen können nur einen begrenzten Schutz bieten, wenn Mitarbeiter oder externe Dienstleister auf Daten zugreifen und diese missbrauchen können.

Kopfzerbrechen bereitet Sicherheitsexperten auch der unbesorgte Umgang mit Daten in den „Mitmach“-Anwendungen des Web 2.0, insbesondere in den immer populärer werdenden Social Networks. Bedenkenlos geben Anwender in ihren Benutzerprofilen detailliert private Informationen preis. Dabei vergessen sie oft, dass Informationen im Netz praktisch jedermann zugänglich sind und es auch bleiben.

Zur Manipulation von Systemen und ihrer Absicherung auf technischer Basis ist also eine weitere Komponente hinzugekommen. Der vorliegende Bericht zeigt deutlich, dass Angreifer zunehmend psychologisches Geschick beweisen. Sie fingieren Mails, die den Nutzer dazu verleiten sollen, auf darin enthaltene Links zu klicken und infolgedessen unbemerkt Programme zu installieren oder vertrauliche Informationen preiszugeben. Auch hier ist das Web 2.0 mit dynamischem und vom Nutzer selbst erzeugtem Inhalt den Kriminellen eine große Hilfe.

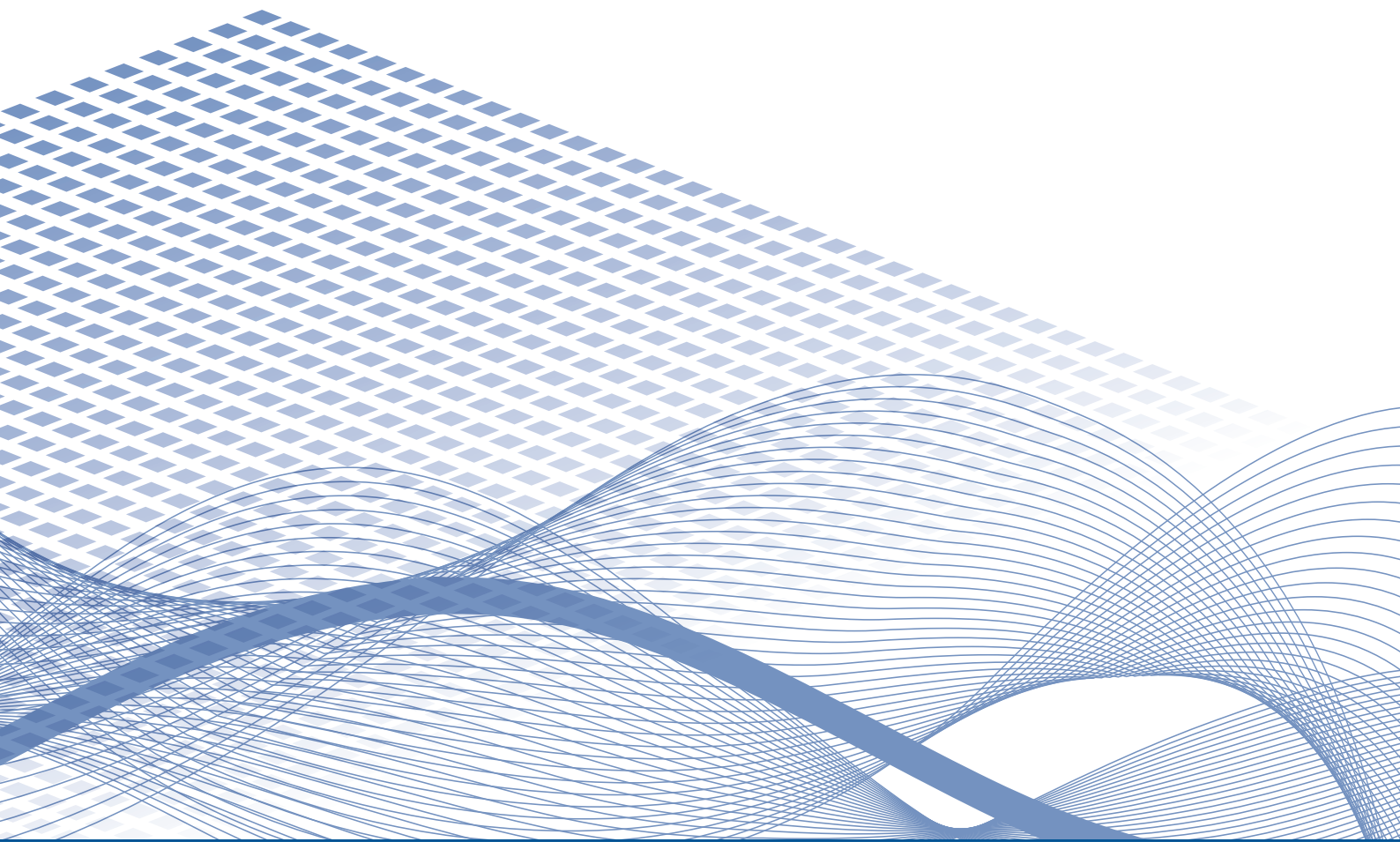



Festzuhalten bleibt: Die Gefahr durch Online-Kriminalität steigt. Schutzmaßnahmen muss jeder Einzelne treffen und den für sich nötigen Grad der Absicherung festlegen. Daher ist eine umfangreiche und kontinuierliche Sensibilisierung der Internetnutzer und -nutzerinnen unerlässlich.

Der dritte Bericht zur Lage der IT-Sicherheit in Deutschland gibt einen Überblick über aktuelle Risiken und Gefahren. Er prognostiziert die Entwicklung potenzieller Bedrohungen, die auch durch den Einsatz innovativer Technologien und ihrer Anwendungen begünstigt werden. Neben Erhebungen des BSI werden Analysen von Partnern aus dem öffentlichen und privaten Sektor sowie Studien von IT-Dienstleistern für den Bericht herangezogen.



IT-Sicherheitsbewusstsein und IT-Sicherheitskompetenz in der Gesellschaft





3 IT-Sicherheitsbewusstsein und IT-Sicherheitskompetenz in der Gesellschaft

Kaum ein Bürger, eine Behörde oder ein Unternehmen zählt heute noch zu den so genannten Offlinern, das heißt zu denen, die das Internet nicht nutzen. Das Thema IT-Sicherheit ist darum so aktuell wie nie. Dennoch ist die Abhängigkeit von der Verfügbarkeit, Integrität, Authentizität und Vertraulichkeit der jeweiligen Technik nicht überall gleich. Die Folgen fehlender oder unzureichender IT-Sicherheitsmaßnahmen treffen jeden anders. Außerdem beeinflussen Faktoren wie die eigene Technikaffinität und -akzeptanz sowie die eigenen Sicherheitsbedürfnisse und -kenntnisse das Bewusstsein und die Kompetenz der verschiedenen gesellschaftlichen Gruppen.

3.1 Bürger

Die Zahl der privaten Internetnutzer steigt weiterhin, während der Anteil der Offliner im Jahr 2008 erstmals unter 30 Prozent sank.[1] Breitbandanschlüsse sind mittlerweile die Norm. Mit diesen Entwicklungen einher geht eine stärkere Nutzung des Internets für Aktivitäten und Transaktionen des täglichen Bedarfs. Nach wie vor ist E-Mail-Kommunikation der am meisten genutzte Dienst im Netz. Mehr als die Hälfte der Anwender nutzt das Internet mittlerweile aber auch, um einzukaufen und um Bankgeschäfte zu erledigen.[2]

Online-Nutzung

Private E-Mails versenden und empfangen	88,9%
Recherche in Suchmaschinen / Web-Katalogen	88,0%
Nachrichten zum Weltgeschehen	64,6%
Online-Einkaufen bzw. -Shoppen	62,0%
Regionale oder lokale Nachrichten	56,4%
Online-Banking	54,8%
Messenger	39,7%
Chats und Foren	37,8%

Quelle: AGOF e.V.

Abbildung 1: Thematische Schwerpunkte der Internetnutzung in Deutschland [2]

Gerade beim Umgang mit sensiblen Daten, wie dies beim Online-Banking und E-Commerce der Fall ist, muss eine gute Sicherheitsausstattung vorhanden sein, um die vertraulichen Informationen zu schützen. Immerhin sind fast vier Millionen Deutsche bereits Opfer von Computerkriminalität geworden und erlitten einen finanziellen Schaden, beispielsweise durch Viren, bei Online-Auktionen oder beim Online-Banking.[3] Und auch wenn die Mehrheit der Nutzer nach eigener Einschätzung bislang keinen spürbaren Schaden erfahren hat, so ist die Gefahr durch Computerschädlinge nicht zu unterschätzen. Oftmals sind Manipulationen am Rechner für den Nutzer nicht ohne weiteres zu erkennen.

Studien zeigen, dass sich der positive Trend aus dem Lagebericht 2007 fortgesetzt hat: Das Thema Sicherheit ist mittlerweile für die meisten Anwender wichtig. Dabei zeigen deutsche Nutzer im internationalen Vergleich ein hohes Sicherheitsbedürfnis.[4] In der Folge wird auch die Umsetzung von Sicherheitsmaßnahmen konsequenter vorangetrieben als noch vor ein bis zwei Jahren. So ist bei fast allen Sicherheitstechniken ein Nutzungsanstieg zu verzeichnen. Firewall und Virenschutzsoftware sind heute weitgehend gängige Schutzmaßnahmen. Auch die Häufigkeit mit der ein Betriebssystem aktualisiert wird, hat deutlich zugenommen: Die Zahl der Nutzer, die eine Aktualisierung sofort bei Erscheinen eines Updates vornehmen, ist innerhalb eines Jahres um 17,6 Prozentpunkte gestiegen und liegt nun bei 74,1 Prozent.[1]

Die rasante Zunahme zeitkritischer Sicherheitslücken spiegelt sich im veränderten Informationsverhalten der Internetnutzer wider. Anstelle von Computerzeitschriften oder Bekannten liegen nun Newsletter als Informationsquelle bei aktuellen Sicherheitsproblemen vorn.[1] Anwender haben somit die Notwendigkeit zeitnaher und gezielt aufbereiteter Informationen erkannt.

Die bloße Implementierung technischer Sicherheitsmaßnahmen allein reicht allerdings langfristig nicht aus. Wenn es um Datenschutz geht, ist auch das Verhalten der Nutzer von großer Bedeutung. Es zeigt sich nämlich deutlich, dass selbst Personen, die regelmäßig die Sicherheitseigenschaften ihres PCs kontrollieren und updaten, mit vertraulichen Daten inflationär umgehen. Das Thema Web 2.0 gehört mittlerweile fest zum Alltag derzeit noch vorwiegend jüngerer Internetnutzer. Social Networks boomen und verzeichnen mehrere Millionen Mitglieder. Auch Nutzer, die ansonsten viel Wert auf (Daten-)Sicherheit legen, geben auf diesen Plattformen bereitwillig persönliche Informationen wie Postanschrift, E-Mail-Adresse, Geburtsdatum und Hobbys preis. Dass sich hinter einem Kontakt aus einem Social Network auch ein Hacker oder Spammer verstecken könnte, bedenken die Wenigsten. Für Cyberkriminelle ist es somit ein Leichtes, auf diese Weise potenzielle Opfer auszuspionieren und gezielt anzugreifen. Das Thema Web 2.0 wird daher künftig eine wichtige Rolle bei der Aufklärung und Sensibilisierung der Bürger spielen.

3.2 Wirtschaft

Um wettbewerbsfähig zu sein und effizient arbeiten zu können, stehen Unternehmen in Deutschland heute vor der Herausforderung, neue Informationstechnik einzusetzen. Bereits im Lagebericht 2007 wurde angesichts immer neuer Bedrohungsszenarien, mit denen die eingesetzten Systeme konfrontiert werden, der Bedarf nach einem auf oberster Leitungsebene initiierten Sicherheitsprozess thematisiert.

Insgesamt lässt sich sagen, dass IT-Sicherheit mittlerweile tatsächlich systematischer angegangen wird: Der Prozentsatz der Unternehmen, die planen, in 2008 Projekte zum Sicherheitsmanagement aufzusetzen, ist um 20 Prozent gestiegen.[5]

73 Prozent der IT-Sicherheitsbeauftragten in Unternehmen und Verbänden betonen mittlerweile die Wichtigkeit eines sicheren IT-Betriebes, um reibungslose Arbeitsabläufe in ihrer Organisation zu gewährleisten. Im Jahr 2005 waren es lediglich 66 Prozent.[6] Als Hauptgrund für Sicherheitsinvestitionen wird ein potenzieller Schaden basierend auf einer Risikobewertung angeführt. Jedoch auch die im Lagebericht 2007 vorhergesagte Zunahme gesetzlicher Vorgaben bezüglich Haftungsregelungen und Kreditvergabe wird als Grund für Investitionen im Sicherheitsbereich genannt.[7]

Sicherheitsinvestitionen

Potenzieller Schaden nach Risikobewertung	55,3%
Potenzielle Haftung	53,2%
Forderung von Behörden / der Gesetze	50,6%
Sicherheit = Unternehmenswert / Verbesserung des Images	37,6%
Allgemein übliche Branchenpraxis	34,6%
Anforderungen von Partnern / Zulieferern / Händlern usw.	32,9%
Basel II / Kreditvergabe / SOX / MARISK	22,2%
Potenzielle Auswirkung auf die Einnahmen	22,0%
Zuvor entstandener Schaden	14,3%
Sonstiges	0,9%
Weiß nicht / Kein Kommentar	11,3%

Quelle: InformationWeek

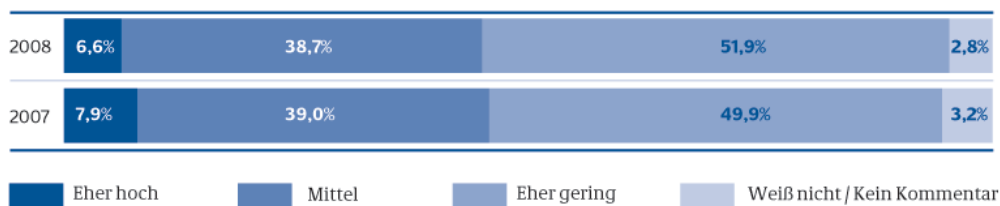
Abbildung 2: Gründe für Sicherheitsinvestitionen in deutschen Unternehmen [7]

Vor diesem Hintergrund ist es nicht verwunderlich, dass der Markt für Security-Lösungen und -Dienstleistungen zwischen 2006 und 2009 ein durchschnittliches jährliches Wachstum von 12,7 Prozent aufweist. Vom Marktvolumen in Höhe von 4,44 Milliarden Euro entfallen im Jahr 2008 in Deutschland 2,34 Milliarden Euro auf Security-Hardware und -Software sowie 2,1 Milliarden Euro auf Security-Dienstleistungen.[8]

Dabei wollen mehr als die Hälfte der Unternehmen das Vorjahresniveau bei den Ausgaben für die Verbesserung ihrer Sicherheitsarchitekturen halten und 42 Prozent der Unternehmen mehr investieren. Im Vergleich zum Gesamtbudget für IT-Ausgaben zeigen die Budgets für IT-Sicherheit allerdings eine andere Gewichtung. 54 Prozent befragter Unternehmen wollen weniger als fünf Prozent ihres Gesamtbudgets für IT-Sicherheit investieren. Nur knapp zwei Prozent der Unternehmen investiert mehr als zehn Prozent des gesamten IT-Budgets. Im Jahr 2006 waren es noch fünf Mal so viele. Andere Investitionsbereiche – vor allem solche, die die Kundenbeziehungen verbessern – sind derzeit vorrangig.[5]

Insgesamt aber scheint das Sicherheitsempfinden auf Unternehmensseite gestiegen zu sein. Laut einer Umfrage wird das Sicherheitsrisiko im Unternehmen im Jahr 2008 als geringer eingeschätzt als im Jahr zuvor.[7]

Einschätzung des Sicherheitsrisikos



Quelle: InformationWeek

Abbildung 3: Einschätzung des Sicherheitsrisikos in deutschen Unternehmen [7]

In den vergangenen Jahren sahen die Unternehmen ihre Daten vor allem durch Fehler oder mangelnde Sensibilisierung von Mitarbeitern gefährdet. Erst an zweiter Stelle standen Schadsoftware und Angriffe von außen. Die Erwartung, dass sich diese Reihenfolge zukünftig ändert, bestätigte sich 2008. Hacking und vorsätzliche Manipulation von IT-Systemen haben an Bedeutung stark zugenommen.[9]

Kritische Infrastrukturen (KRITIS)

Bei den Betreibern der so genannten Kritischen Infrastrukturen können IT-Sicherheitsbewusstsein und -kompetenz sowohl auf Managementebene als auch in der Umsetzung durchweg als hoch eingeschätzt werden. Dies spiegelt sich auch im Umsetzungsplan KRITIS (UP KRITIS) wider, der durch Experten aus etwa 30 Unternehmen Kritischer Infrastrukturen gemeinschaftlich mit Bundesbehörden erarbeitet und 2007 vom Bundesministerium des Innern (BMI) veröffentlicht wurde. Die an der Erstellung des UP KRITIS beteiligten Unternehmen und Organisationen haben sich die Aufgabe gestellt, die dort gegebenen Empfehlungen zu Sicherheitsmaßnahmen in Kritischen Infrastrukturen umzusetzen und weitere Maßnahmen zu entwickeln. Ein besonderer Fokus liegt auf den Empfehlungen für unternehmensübergreifende Maßnahmen, die eine intensive und vertrauensvolle Zusammenarbeit über Unternehmens- und Branchengrenzen hinaus erfordern (vgl. Kapitel 8.2).

3.3 Verwaltung

Ein moderner Staat braucht eine innovative und leistungsfähige Verwaltung, welche die zeitgemäße Technik sicher einsetzt. Als Anbieter vielfältiger elektronischer Dienstleistungen kommen neue verantwortungsvolle Herausforderungen auf die öffentlichen Verwaltungen zu. Hier sind zum Beispiel alle Prozesse zu nennen, die gehobene Ansprüche an ein sicheres und modernes Identitätsmanagement stellen, wie beispielsweise die neue Gesundheitskarte oder die Zusammenführung von kommunalen Melderegistern. Die Erwartungen der Bürger an die Dienstleistungen der Verwaltung sind vielfältig. Sie müssen verfügbar sein, sollten ein Höchstmaß an Verlässlichkeit bieten und alle Informationen ohne Ausnahme vertraulich behandeln. Außerdem sind die Daten auf den Kommunikationswegen zwischen den Behörden gegen unautorisierten Zugriff zu schützen. Gleichzeitig müssen diese Dienstleistungen immer wieder an moderne Technologien oder neue Standards angepasst werden, um die Bürgernähe und Benutzerfreundlichkeit aufrecht zu erhalten.

Die grundsätzliche Erkenntnis, dass der Faktor IT-Sicherheit nicht vernachlässigt werden darf, hat sich in den vergangenen Jahren sehr wohl durchgesetzt. Dies lässt sich auf bekannt gewordene Fälle des Missbrauchs, insbesondere im Bereich des Datenschutzes zurückführen und begründet die gehobene Erwartungshaltung gegenüber der Sicherheit von Verwaltungsdienstleistungen. Nicht zuletzt aus diesem Grund wurde Ende 2007 für den Bereich der Bundesverwaltung mit dem Umsetzungsplan Bund (UP Bund) eine – zwischen sämtlichen Ressorts abgestimmte – Basis zur Implementierung und Umsetzung von IT-Sicherheit geschaffen. Infolgedessen verändert sich die Umsetzung von IT-Sicherheit in den Verwaltungen von einer Vielzahl von Einmal-Aktionen hin zu einem fortwährenden Prozess, der von qualifiziertem und autorisiertem Personal aufrechterhalten werden soll. Trotz einer objektiven Verbesserung der Situation sind weiterhin Schwierigkeiten erkennbar. Fakt ist, dass bei Entscheidungsträgern in der Verwaltung die Sensibilität in Bezug auf IT-Sicherheit weiterhin erhöht werden muss. Oftmals werden noch nicht genügend finanzielle Ressourcen bereitgestellt. Des Weiteren müssen personelle Maßnahmen getroffen werden, um den IT-Sicherheitsprozess organisatorisch aufrecht zu erhalten. Häufig fehlt es dafür noch an qualifiziertem Personal.



Schwachstellen und Bedrohungen von IT-Systemen



4 Schwachstellen und Bedrohungen von IT-Systemen

4.1 Sicherheitslücken

Komplexe Produkte wie Software enthalten naturgemäß Fehler. Dadurch entstehende Sicherheitslücken können von Angreifern mit Exploits ausgenutzt werden.

Die Anzahl neu entdeckter Sicherheitslücken ist im Jahr 2007 im Vergleich zu den Vorjahren leicht zurückgegangen. Für das Jahr 2008 zeichnet sich zum Beobachtungszeitpunkt Ende Oktober jedoch wieder ein Anstieg auf das Niveau von 2006 ab. Wie in den Vorjahren eignete sich rund die Hälfte der in den Jahren 2007 und 2008 analysierten neuen Schwachstellen dazu, Benutzer- oder sogar Administratorrechte zu erlangen.[10]

Der in den letzten Jahren konstante Trend der Zunahme von Sicherheitslücken, die von einem entfernten Angreifer ausgenutzt werden können, hat sich weiter bestätigt: Über drei Viertel der im Jahr 2008 neu entdeckten Schwachstellen können von einem entfernten Angreifer ausgenutzt werden. Für rund die Hälfte der neu gemeldeten Schwachstellen wurde von den Herstellern der Produkte kein Update zur Behebung des Sicherheitsproblems bereitgestellt.[10]

Der Zeitraum zwischen dem Bekanntwerden einer neuen Sicherheitslücke und der Veröffentlichung eines Exploits ist oft zu kurz, um notwendige Programmupdates zur Verfügung zu stellen oder andere Schutzmaßnahmen zu entwickeln. Wie das BSI im Lagebericht 2007 prognostizierte, ist seitdem ein deutlicher Anstieg der so genannten Zero-Day-Angriffe zu verzeichnen. Bei dieser Art von Angriffen wird eine Sicherheitslücke noch vor oder am gleichen Tag der öffentlichen Bekanntmachung ausgenutzt.

In den letzten Jahren haben Nutzer offenbar zunehmend erkannt, wie wichtig regelmäßig installierte Betriebssystem-Updates sind. Angreifer reagieren darauf und nutzen für ihre Angriffe vermehrt Schwachstellen in weit verbreiteter Anwendungssoftware aus. Diese Vorgehensweise bietet den Angreifern entscheidende Vorteile: So stellen viele Entwickler von Anwendungssoftware Updates nicht kurzfristig zur Verfügung. Hinzu kommt, dass die Software häufig nicht über automatische Update-Mechanismen verfügt und Anwender mit der manuellen Installation oft überfordert sind. Außerdem sind sich viele Nutzer der Tatsache nicht bewusst, dass auch für eingesetzte Anwendungssoftware Updates einzuspielen sind.

Zunehmende Gefahr geht von den so genannten Drive-by-Downloads aus. Angreifer manipulieren dabei vermehrt auch seriöse Webseiten, um vom Nutzer unbemerkt Schadcode auf den PC zu schleusen. Ausgenutzt werden hierzu Sicherheitslücken im Webbrowser oder in installierten Zusatzkomponenten (Plug-Ins). Nach Erkenntnissen des BSI existieren die meisten Schwachstellen im Zusammenhang mit Webbrowsern in ActiveX-Steuerelementen, die zur Darstellung von Aktiven Inhalten verwendet werden.


4.2 Schadprogramme

Die Einteilung von Schadprogrammen in verschiedene Kategorien wie Viren, Würmer, Trojanische Pferde oder Bots wird zunehmend schwierig. Die meisten Schadprogramme sind modular aufgebaut und verfügen über mehrere Schadfunktionen. So kann beispielsweise ein Trojanisches Pferd über Backdoor- und Spywarefunktionen verfügen, einen Keylogger verwenden und den befallenen Rechner zusätzlich an ein Bot-Netz anschließen. Zudem verfügen die meisten Schadprogramme über Updatefunktionen, so dass neue Programme oder Tarnmechanismen jederzeit nachgeladen werden können. Bot-Rechner, die mehrfach am Tag mit Updates versorgt werden, sind daher Standard.

Es ist mittlerweile sehr einfach, bösartige Programme zu erstellen oder vorhandene Exemplare an die jeweiligen kriminellen Bedürfnisse anzupassen. Aussagen über die genaue Anzahl von Schadprogrammen sind dadurch inzwischen wertlos geworden. Je nach Klassifikation und Zählweise unterscheiden sich die Werte der IT-Sicherheitsfirmen erheblich. In einem sind sich jedoch alle einig: Es gibt Millionen von Schadprogrammen, deren Anzahl immer schneller wächst. Jeden Monat kommen Zehntausende hinzu.

Die Herstellung und der Einsatz von Schadprogrammen verhelfen organisierten Kriminellen zu Gewinnen in Milliardenhöhe und sind fester Bestandteil in ihrer „Wertschöpfungskette“.

Obwohl immer mehr Schadsoftware im Umlauf ist, werden einzelne Schadprogramme jetzt gezielter eingesetzt als früher und nicht mehr wahllos an möglichst viele Opfer verteilt. Je geringer die Verbreitung eines bestimmten Schadprogramms ist, desto niedriger ist die Wahrscheinlichkeit, dass es den Herstellern von Virenschutzprogrammen rasch bekannt wird und damit über das Update der Erkennungs-Signaturen auch von einem Schutzprogramm erkannt wird. Die Einsatzdauer eines Schadprogramms lässt sich so verlängern.



Wurden vor zwei Jahren die meisten Schadprogramme per E-Mail verschickt, erfolgt die Verbreitung inzwischen in großer Zahl über präparierte Webseiten (Drive-by-Downloads). Untersuchungen zufolge wurden im Zeitraum von Januar bis März 2008 durchschnittlich 15.000 infizierte Webseiten pro Tag entdeckt. Davon gehörten 79 Prozent zu an sich harmlosen Internetangeboten.[11] Die meisten Angriffe erfolgen dabei über das Einschleusen von so genannten Inlineframes, welches mit geringem Aufwand (zum Beispiel über SQL-Injection) automatisiert möglich ist, wenn die Webseite eine Schwachstelle enthält. Ein einziger Angreifer kann auf diese Weise mehrere Tausend Webseiten innerhalb weniger Stunden infizieren. In den meisten Fällen müssen dazu Aktive Inhalte (wie JavaScript) auf dem Rechner des Webseitenbesuchers freigeschaltet sein, damit die Schadprogramme eingeschleust und ausgeführt werden können.

Insbesondere die Autoren von Trojanischen Pferden und Bots, die sich mit hoher krimineller Energie einen finanziellen Vorteil verschaffen wollen, verbessern ständig ihre Schutzmechanismen, um die Erkennung und Analyse des Schadcodes zu erschweren. Die meisten Schadprogramme schützen sich inzwischen mit kryptographischen Verfahren und passen ihr Verhalten an – je nachdem, ob sie in einer typischen Analyseumgebung oder auf einem echten Opferrechner ausgeführt werden.

Bislang arbeitet Schutzsoftware hauptsächlich signaturbasiert, das heißt, ein Virenschutzprogramm erkennt nur bereits bekannte Schadprogramme. Diese Technik ist an ihre Grenzen gestoßen, so dass intensiv an Technologien gearbeitet wird, die neue Schadprogramme auch an ihren Eigenschaften bzw. ihrem Verhalten erkennen können. Das Problem dabei: Verhaltensbasierte Erkennungsverfahren führen immer zu einer höheren Anzahl von unberechtigten Alarmen (so genannte false positives). Dies ist für die Nutzer der Schutzsoftware jedoch problematisch, insbesondere, wenn dadurch fälschlicherweise wichtige Betriebssystemprogramme deaktiviert oder sogar gelöscht werden. Auf Angreiferseite wird beständig daran gearbeitet, die Tarnmechanismen zu verbessern. Beispielsweise ist zukünftig mit Schadprogrammen zu rechnen, die das Betriebssystem in eine virtuelle Umgebung verschieben, das heißt sich zwischen die Hardware und das Betriebssystem installieren, so dass sie von herkömmlichen Schutzprogrammen nicht mehr entdeckt werden können.

4.2.1 Trojanische Pferde


Trojanische Pferde installieren sich heimlich und bringen einen einzelnen Rechner unter die Kontrolle eines Angreifers. Sie sind das wichtigste Werkzeug, um Passwörter zu stehlen oder ein Opfer gezielt auszuspionieren. Die Aussagen aus dem Lagebericht 2007 über die zunehmende Anzahl gezielter Angriffe mit multifunktionalen Trojanischen Pferden zu Spionagezwecken sind unverändert gültig. In den Jahresberichten der Verfassungsschutzbehörden des Bundes und der Länder finden sich Informationen über Art und Urheber elektronischer Angriffe auf Wirtschaftsunternehmen und Behörden durch ausländische Nachrichtendienste. Wurden dabei früher hauptsächlich zentrale Server einer Behörde oder eines Unternehmens angegriffen, um das dahinter liegende Netz auszuspionieren, haben sich die gezielten Angriffe auf einzelne Arbeitsplatzrechner verlagert. Durch geschicktes Social Engineering werden IT-Anwender dazu gebracht, eine präparierte E-Mail oder Webseite zu öffnen bzw. einen manipulierten Datenträger (zum Beispiel USB-Stick) anzuschließen. Bei Angriffen über manipulierte E-Mail-Anhänge werden aufgrund der weiten Verbreitung am häufigsten Microsoft Office-Dateien (wie Word oder PowerPoint) oder PDF-Dateien missbraucht. Für das Opfer ist die Manipulation in der Regel nicht zu erkennen.

Klassische Schutzmaßnahmen wie Virenschutzprogramme und Firewalls sind nicht mehr ausreichend, um einen wirksamen Schutz gegen die aggressiven Methoden der Wirtschaftsspionage zu erreichen. Weitergehende IT-Sicherheitsmaßnahmen sind unumgänglich.

4.2.2 Spyware

Spyware-Programme spionieren das Surf-Verhalten einer Person im Internet aus, um Benutzerprofile zu erstellen. Diese werden dann entweder vom Spyware-Ersteller selbst genutzt oder an kommerzielle Firmen verkauft, damit diese zielgerichtet Werbeeinblendungen platzieren können.

Besonders gefährlich ist es, wenn die Spyware auch Anmeldedaten wie Benutzername oder Passwort heimlich mitprotokolliert und dann überträgt. Mit diesen Daten kann ein Identitätsdiebstahl ermöglicht werden. Zur Entfernung von Spyware müssen spezielle Anti-Spyware-Programme eingesetzt werden, da nur wenige Virenschutzprogramme dies ebenfalls leisten. Aus juristischer Sicht wird Spyware nicht als Schadprogramm, sondern als „möglicherweise unerwünschte Software“ bezeichnet.



Die Bedrohung durch Spyware ist in den letzten Jahren gestiegen, was hauptsächlich darauf zurückzuführen ist, dass die Grenzen zwischen Spyware-Programmen und Trojanischen Pferden mittlerweile fließend geworden sind. Beide Arten von Schadprogrammen werden vorwiegend über präparierte Webseiten oder Bot-Netze verteilt.

4.3 DoS-Angriffe

Nachdem im zweiten Quartal 2007 der „Estland-Vorfall“ das Thema der DoS-Angriffe schlagartig in das Blickfeld der Öffentlichkeit rückte, folgten weitere massive DoS-Angriffe, die während des Georgien-Konflikts im Herbst 2008 einen vorläufigen Höhepunkt erreichten.

Ein Denial-of-Service-Angriff (DoS-Angriff) bezeichnet allgemein den bewussten Versuch, die Verfügbarkeit eines IT-Systems zu stören. Im Extremfall wird dadurch jegliche Nutzung über einen längeren Zeitraum hinweg verhindert. Der dadurch entstehende Schaden hängt vom Einsatzzweck der gestörten IT-Anwendung ab und reicht von Produktionsausfall, Umsatzeinbußen und Reputationsverlust bis hin zu Versorgungsengpässen bei Einzelpersonen oder Unternehmen. Ein DoS-Angriff kann somit zu einer existenziellen Bedrohung der Betroffenen werden.

Bereits im Lagebericht 2007 wurde auf die Zunahme von Distributed-Denial-of-Service-Angriffen (DDoS-Angriffe) hingewiesen. Dieser Trend hat sich bis heute fortgesetzt. Mithilfe vieler verteilter (distributed) Client-Systeme wird eine hohe Lastsituation erzeugt, mittels der die Datenverbindungen bzw. die beteiligten IT-Systeme effektiv blockiert werden.

Doch nicht jede Verfügbarkeitsstörung ist unmittelbar auf einen gezielten DoS-Angriff auf die eigene Organisation zurückzuführen. Vielfach werden IT-Anwendungen verschiedenster Organisationen zentral durch Dienstleistungsunternehmen betreut oder IT-Infrastrukturkomponenten gemeinsam genutzt. Massive Angriffe auf ein Ziel wirken sich dann automatisch auf benachbarte Bereiche aus.

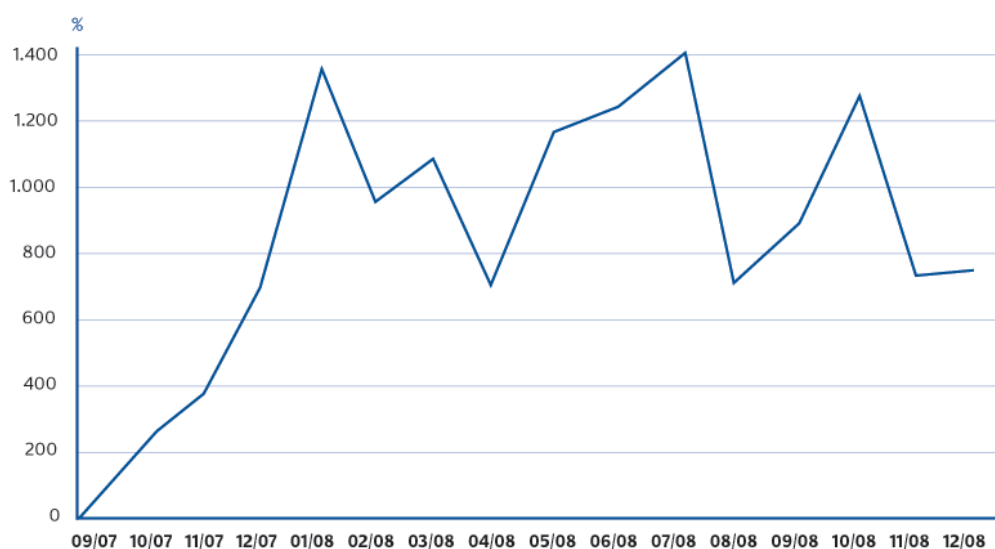
DoS-Angriffe sind ein altbekanntes Phänomen, nach wie vor ist die Bedrohung ungebrochen hoch. Neben den klassischen Motiven wie der Schädigung von Konkurrenten, dem Erpressen von Schutzgeldzahlungen oder die Demonstration der eigenen Überlegenheit nehmen ideologisch bzw. politisch motivierte Aktionen weiter zu. Sowohl der Estland-Vorfall als auch der Georgien-Konflikt verdeutlichten dies in drastischer Weise.

Grundsätzlich stellen DoS-Angriffe eine Bedrohung für jegliche IT-Systeme dar. Abhängig vom Schutzbedarf besonders sensibler Systeme sollten umfassende Vorsorgemaßnahmen und Notfallplanungen vorbereitet werden, um im Fall eines Angriffs die Auswirkungen zu mindern und den Regelbetrieb schnellstmöglich wieder aufnehmen zu können.

4.4 Unerwünschte E-Mails (Spam)


Wie erwartet, ist das Spam-Aufkommen in den vergangenen zwei Jahren weiterhin erheblich gestiegen. Die unerwünschte Nachrichtenflut überschwemmt tagtäglich die Postfächer der Internetnutzer. Am Netzübergang der Bundesbehörden konnte festgestellt werden, dass von 100 empfangenen Mails im Durchschnitt gerade einmal 1,5 Mails gewollt sind.[6] Bei unzureichenden Filtermethoden kann der Erhalt von massenhaft versendeten Spam-Mails unvermittelt in einen DoS-Angriff übergehen.

Entwicklung unerwünschter E-Mails



Quelle: BSI

Abbildung 4: Prozentualer Anstieg des Spam-Aufkommens in der Bundesverwaltung [6]



Mithilfe von immer leistungsfähigeren Anti-Spam-Methoden wird versucht, die Flut von Spam-Mails einzudämmen. Ob die Spam-Erkennung über die Absenderadressen, den Inhalt oder über die Metadaten durchgeführt wird, ändert jedoch nichts an der Tatsache, dass auch die Methoden der Spam-Versender immer professioneller werden.

Die Inhalte der Mails sind vielfältig und werden immer individueller. Die Empfänger werden zunehmend persönlich angesprochen. Der Mail-Inhalt ist häufig nicht sofort als Spam-Text erkennbar, da sich die sprachliche Qualität sehr verbessert hat. Die Inhalte reichen von Angeboten zu Online- und Gewinnspielen über Medikamente bis hin zu finanziellen Lockangeboten sowie Job-Offerten. Hinzu kommen Mails mit gefährlichen Inhalten.

Um vor allem die Inhalts-Spam-Filter noch wirkungsvoller zu umgehen, wird auf so genannte Container- oder Attachment-Spams zurückgegriffen. Dabei wird eine Bild-, MP3-, Excel- oder Zip-Datei im Anhang der Mail versendet. Der Trend bei dieser Methode ist der Versand von Dateien im PDF-Format, die mit dem Adobe Reader betrachtet werden können.

Werbemails können lästig sein. Spam-Mails, die mit betrügerischer Absicht versendet werden, sind dazu noch gefährlich. Dazu gehören E-Mails, die auf Phishing-Seiten verweisen, finanzielle Lockangebote sowie Mails, die zum Spenden animieren sollen oder mit schädlichen Anhängen oder Links versehen sind. Für Kriminelle ist der Spam-Versand ein lohnendes Geschäft, denn dem Versender selbst entstehen so gut wie keine Kosten.

Die finanzielle Last trägt vor allem der Nutzer in Form von Arbeitszeitausfällen, unnötigem Datentransfer, den Folgen von DoS-Angriffen oder als Opfer eines Betrugs.

4.5 Bot-Netze

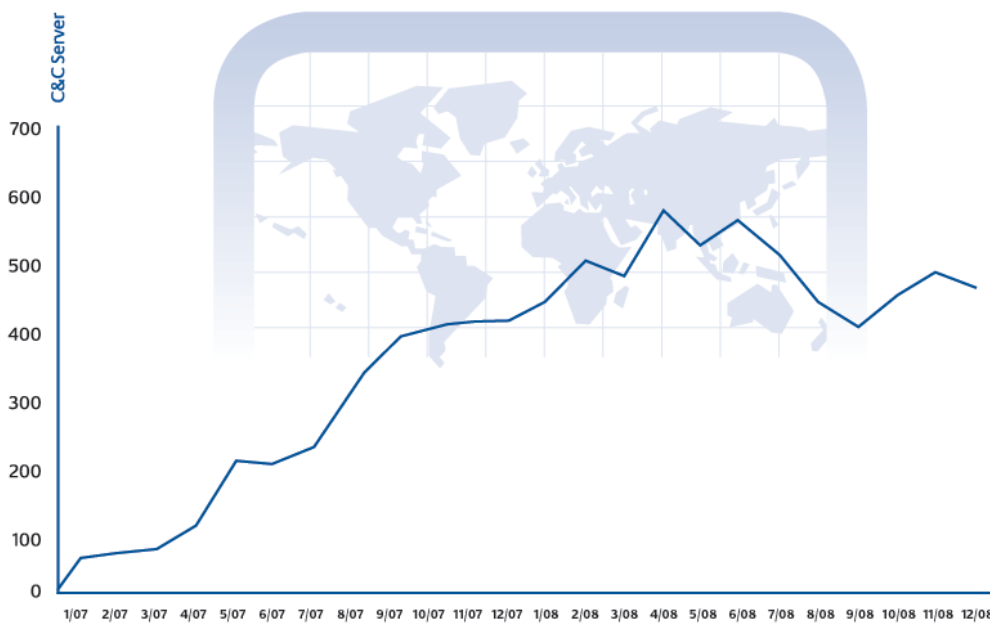
Die Infektion eines PCs mit Bots erfolgt zum Beispiel unter Ausnutzung bekannter Sicherheitslücken in Systemdiensten und Applikationen. Eine weitere effektive Infektionsmethode ist der Einsatz von Social Engineering, um den Anwender zu einer unbedachten Handlung wie dem Klicken auf bösartige E-Mail-Links bzw. Instant-Messaging-Nachrichten oder der Ausführung von E-Mail-Anhängen zu verleiten. In jüngster Zeit ist außerdem zu beobachten, dass legitime, vertraute und stark frequentierte Webseiten manipuliert werden, um sie für die Verbreitung von Schadcode zu missbrauchen.

Bot-Netze werden für viele illegale Aktivitäten eingesetzt. Dazu gehört der massenhafte Versand unerwünschter E-Mails mit bösartigen Anhängen und Links, aber auch die Aufzeichnung von Tastaturanschlägen (Keylogging), um an persönliche Informationen zu gelangen. Darüber hinaus werden Bot-infizierte Rechner als Ablagestelle für illegale Software missbraucht oder zur Ausführung von gezielten DDoS-Angriffen verwendet.

Ein wichtiger Aspekt bei der Betrachtung von Bot-Netzen ist ihre Kommunikations- und Steuerungsinfrastruktur. In den meisten Fällen erfolgt die Steuerung über einen oder mehrere Command-and-Control-Server (C&C-Server). Zu den Vorteilen eines zentralen Steuerungsmodells mit einem einzelnen C&C-Server gehört die einfache Entwicklung und Administration. Einer der wesentlichen Nachteile für die Angreifer ist jedoch, dass eine Abschaltung dieses Servers dazu führt, dass das Bot-Netz nicht mehr genutzt werden kann. Seit Erscheinen des letzten Lageberichts setzen Kriminelle daher zunehmend auch ausgeklügelte Kommunikationsstrukturen mit Rückfallmechanismen auf mehrere C&C-Server und, aufgrund ihrer ohnehin dezentralen Architektur, P2P-Protokolle ein. In Einzelfällen werden auch Verschleierungstechniken wie Kompression und Verschlüsselung genutzt. Das BSI bestätigt einen Trend von IRC-basierten hin zu HTTP-basierten Bot-Netzen. Im Jahr 2007 wurden im Durchschnitt 267 auf Informationsdiebstahl spezialisierte HTTP-basierte C&C-Server identifiziert. In 2008 waren es 503 C&C-Server im Jahresdurchschnitt. Dies entspricht einer Steigerung um 88,35 Prozent gegenüber dem Vorjahr.[6]

Die hier skizzierte Form der Kriminalität ist Teil einer professionell und international aufgestellten Schattenwirtschaft. Die organisierte Kriminalität nutzt das Internet und die Informationstechnik zunehmend für ihre Zwecke: Im Internet kann man Bot-Netze mieten und sich zum Spam-Versand mit anderen zusam-

Steuerung von Bot-Netzen



Quelle: BSI

Abbildung 5: Anzahl der auf Informationsdiebstahl spezialisierten Command-and-Control-Server 2007 und 2008 [6]

menschließen. Auf Webseiten oder in E-Mails gibt es entsprechende Angebote. Die zunehmende Professionalisierung der Schadsoftware-Autoren und die fortschreitende Kommerzialisierung im Bot-Netz-Umfeld machen das unvermindert hohe Gefährdungspotenzial von Bot-Netzen deutlich. Hinzu kommen außerdem die vielfältigen Einsatz-Szenarien und enorme Schlagkraft von Bot-Netzen: Ein Bot-Netz bestehend aus 1000 Bot-infizierten Rechnern kann beispielsweise die Infrastruktur vieler kleiner Unternehmensnetze lahm legen.

Durch den konsequenten Einsatz traditioneller Sicherheitskonzepte wie Virenschutzsoftware, Desktop Firewalls, regelmäßige Updates des Betriebssystems und dessen Anwendungen, Konten mit eingeschränkten Rechten für Internet-Anwendungen und vor allem große Sorgfalt im Online-Verhalten kann die Gefahr einer Infektion für private Anwender gesenkt werden. Auch Unternehmen und Behörden können durch die Implementierung organisatorischer und technischer Maßnahmen sowohl die Gefahr einer Infektion reduzieren als auch ihre Netze überwachen und verteidigen.

4.6 Identitätsdiebstahl

Mittels Identitätsdiebstahl versuchen Kriminelle personenbezogene Daten zu missbrauchen, um sich damit einen – meist finanziellen – Vorteil zu verschaffen.

Klassische Phishing-Mails, mit denen Kunden auf gefälschte Webseiten von Kreditinstituten gelockt werden sollen, um dort ihre Online-Banking-Daten preiszugeben, gibt es heute kaum noch. Bereits im Lagebericht 2007 wurde über den zunehmenden Einsatz von Trojanischen Pferden zu Spionagezwecken berichtet. Inzwischen setzen Datendiebe fast ausschließlich Trojanische Pferde ein.

Durch die Einführung verbesserter Sicherheitsmaßnahmen beim Online-Banking wie iTAN- oder mTAN-Verfahren sind die Schäden in diesem Bereich im Jahr 2008 stark zurückgegangen. Die Schadenreduzierung wird jedoch durch neue betrügerische Betätigungsfelder der Kriminellen wieder ausgeglichen.

Während in den letzten Jahren vorwiegend Nutzerdaten für Online-Banking und Kreditkarten für betrügerische Finanztransaktionen missbraucht wurden, werden mittlerweile nicht mehr nur kurzfristige Zugangs- und Transaktions-Daten gesammelt. Informationen zur Identität wie etwa Geburtsdatum, Anschrift und Führerscheinnummern sind ebenfalls Ziel der Angreifer. Mit den gewonnenen Daten werden nunmehr kriminelle Aktivitäten im Bereich von E-Commerce-Angeboten durchgeführt. Bereits jetzt resultieren daraus weltweit Schäden in Milliardenhöhe – mit steigender Tendenz.

Maßnahmen der Bundesregierung zur Gewährleistung einer gesicherten elektronischen Identität und zum Schutz vor Identitätsdiebstahl sind Projekte, die eine verbindliche Authentisierung von Bürgerinnen und Bürgern sowie Anbietern von Diensten in der elektronischen Welt ermöglichen (vgl. Kapitel 6.2).

Identitätsdiebstahl wird aber nicht nur durch die kriminelle Energie von Betrügern, sondern zunehmend auch durch aktives Zutun der Nutzer vereinfacht. Die Popularität von Social Networks, in denen Mitglieder freiwillig eine Vielzahl privater Daten preisgeben, vereinfacht Phishing und Datenmissbrauch erheblich.

Sorge bereiten muss auch, dass die Fälle von Skimming sich in 2008 gegenüber dem Vorjahr nahezu verdoppelt haben.[12] Magnetstreifen-Informationen von Bank- bzw. Kreditkarten werden durch Vorsätze an Geldautomaten ausgelesen, gleichzeitig die PIN-Nummern über verborgene Kameras ausgespäht. Nach Angaben des Bundeskriminalamtes kommen die Täter zu mehr als 90 Prozent aus Rumänien, die gefälschten Karten werden vorwiegend in Rumänien, Spanien, Italien und Frankreich eingesetzt. Die Schadenshöhe durch Skimming liegt derzeit im mittleren zweistelligen Millionenbereich.

4.7 Betrügerische Webangebote

In der Vergangenheit wurden von Betrügern illegale Dialer eingesetzt, um Dritte finanziell zu schädigen. Die Dialer installierten sich unbemerkt auf Computern und stellten über teure Rufnummern Internetverbindungen her. Bereits 2007 wurde darauf hingewiesen, dass aufgrund neuer Verfahren der Telekommunikationsanbieter sowie verschärfter gesetzlicher Regelungen diese Betrugsmasche praktisch nicht mehr vorhanden ist.

Mittlerweile setzt nahezu derselbe Personenkreis daher eine neue Betrugsform ein, um Anwender finanziell zu schädigen. Nutzern werden über vermeintlich kostenlose Informationsangebote im Internet teure Abonnements untergeschoben. Auf seriös erscheinenden Webseiten wird dem Nutzer im Rahmen eines vermeintlich kostenlosen Tests ein Informationsangebot zur Verfügung gestellt. Häufig wird nur im Kleingedruckten erwähnt, dass der Anwender bei Inanspruchnahme des Angebots ein Abo mit längerer Laufzeit abschließt oder aber eine Nutzungsgebühr zu zahlen hat. Die Betrüger arbeiten gezielt mit kleinen Schriftgrößen und schlecht zu unterscheidenden Farben, um die Kostenpflichtigkeit zu verschleiern. Um sich vor derartigen Betrügereien zu schützen, sollte jedes Internetangebot sorgfältig geprüft werden und vor allem die Allgemeinen Geschäftsbedingungen genau durchgelesen werden.

4.8 Kompromittierende Abstrahlung

Eine Möglichkeit, sich unbefugt vertrauliche Informationen zu beschaffen, ist das Empfangen der elektromagnetischen Störstrahlung von IT-Geräten. Jedes elektronische Gerät erzeugt im Betrieb mehr oder weniger starke Störemissionen. Bei IT-Geräten können diese Emissionen auch die gerade verarbeiteten Informationen transportieren. Durch Empfangen und Auswerten dieser Emissionen können so die verarbeiteten Daten aus einiger Entfernung mitgelesen werden. Die Vertraulichkeit der Daten ist dann nicht mehr gegeben. So lässt sich zum Beispiel aus der Störstrahlung von Computerbildschirmen der gerade dargestellte Bildschirminhalt rekonstruieren. Derart informationsbehaftete Störemissionen werden als kompromittierende Abstrahlung bezeichnet. In den vergangenen Jahren wurden analoge Monitore fast vollständig durch digitale Flachbildschirme ersetzt. Damit einhergehend ist die analoge VGA-Schnittstelle der PCs von einer digitalen DVI-Schnittstelle verdrängt worden. Aufgrund der hohen Geschwindigkeit und der speziellen Codierung der Datenübertragung zwischen Rechner und Monitor galt die digitale Schnittstelle lange als relativ unanfällig gegenüber der kompromittierenden Abstrahlung. Aktuelle Untersuchungen haben aber gezeigt, dass auch die Signale der digitalen DVI-Schnittstelle über eine Distanz von mehreren zehn Metern hinweg empfangen und nach einer entsprechenden Aufbereitung sichtbar gemacht werden können.[6] Aufgrund dessen ist es wahrscheinlich, dass das Gefährdungspotenzial durch kompromittierende Abstrahlung in den kommenden Jahren aktuell bleiben wird.

4.9 Materielle Sicherheit, Innentäter, Irrtum und Nachlässigkeit

Auch wenn Unternehmen ihre IT-Infrastruktur gegen externe Angriffe von Computerkriminellen hinreichend abgesichert haben, stellen so genannte Innentäter nach wie vor eine nicht zu unterschätzende Gefahrenquelle für ein Unternehmen dar.

Im verschärften Wettbewerb gewinnt das Thema Wirtschaftsspionage zunehmend an Bedeutung. Moderne Kommunikationsmittel erlauben es, unbemerkt sensible Daten aus dem Unternehmen zu schleusen. Firewall und Antivi-

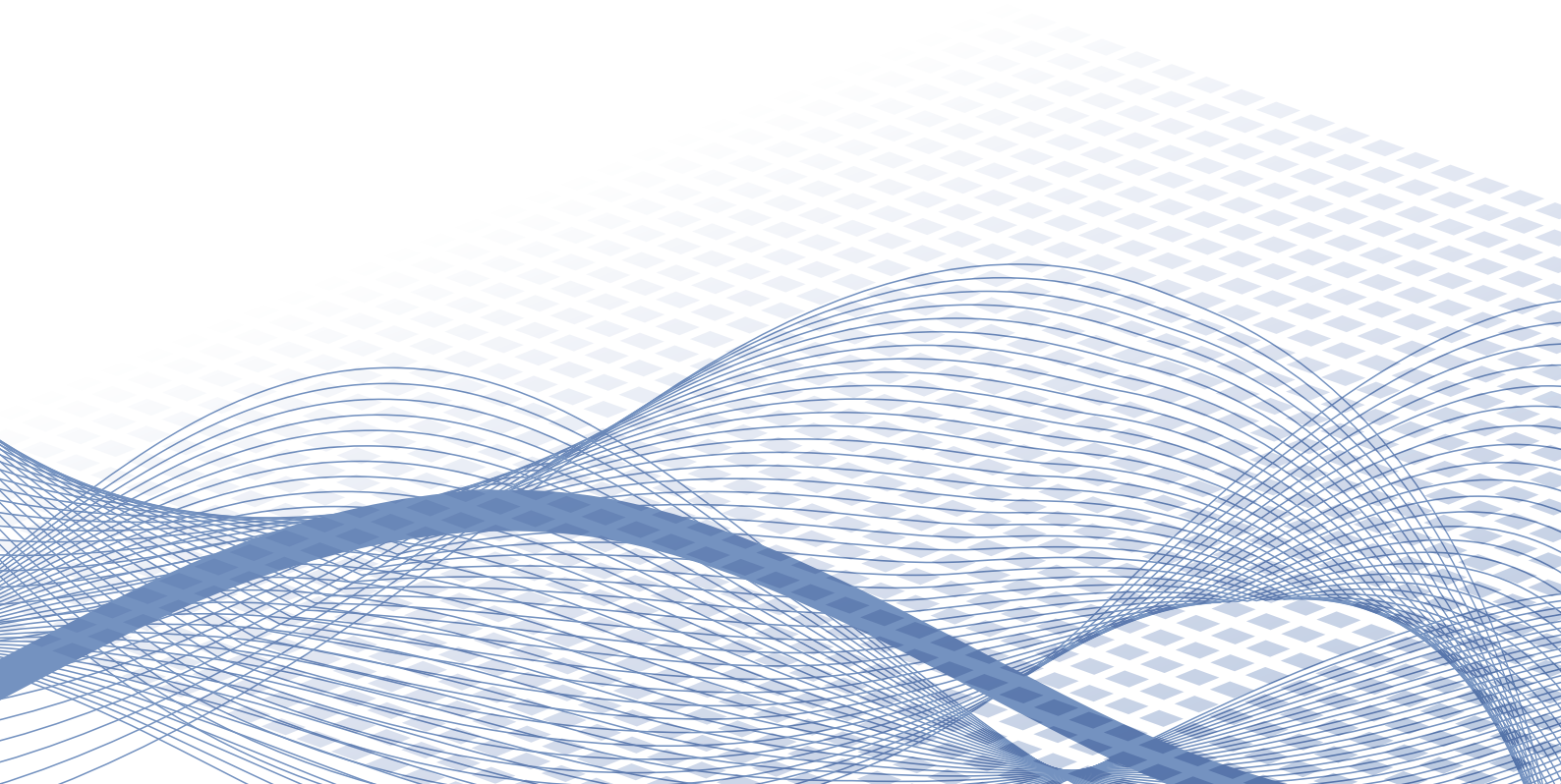
rensoftware bieten hier keinen wirkungsvollen Schutz. Ein Informationsdiebstahl durch die eigenen Mitarbeiter stellt für ein Unternehmen ein hohes Risiko dar. Mit 24 Prozent sind sie die größte Tätergruppe.[13] Finanzielle Anreize oder Rache können Ursachen dafür sein, dass Mitarbeiter zu Tätern werden.

Aber auch schlichtweg nachlässiger oder schlecht geschulter Umgang der Mitarbeiter mit den zur Verfügung gestellten IT-Systemen und -Anwendungen birgt eine große Gefahr für die Vertraulichkeit und Integrität von Daten. Vielfach werden IT-Sicherheitsmaßnahmen aus einem mangelnden Sicherheitsbewusstsein heraus nicht beachtet und umfangreich getätigte, kostspielige Sicherheitslösungen somit unterlaufen. Die im Vordergrund stehenden technischen Vorkehrungen zum Schutz gegen Hacker müssen daher durch Sensibilisierung der Mitarbeiter, aber auch durch strikte Vorgaben zum sensiblen Umgang mit Daten ergänzt werden.

Für Ausgaben an Outsourcing-Dienstleister sagen Unternehmen in den kommenden Jahren gleich bleibende, in einem Drittel der Fälle sogar steigende Budgets vorher.[5] Auch auf diesem Gebiet ist ein hohes Sicherheitsniveau unerlässlich. Zum einen können Daten aus ausgelagerten Bereichen durch Vorsatz oder menschliches Versagen anderen Kunden des Outsourcing-Dienstleisters zugänglich werden. Zum anderen können externe Berater, die Zugang zum Hausnetz haben, an sensible Daten gelangen.

Insgesamt sind zum Schutz der Informationen organisatorische und technische Sicherungsmaßnahmen erforderlich. Angefangen von einer technischen Überwachung durch Zutrittskontrollanlagen zum Objekt oder „sensiblen“ Räumen, der Aufbewahrung der Daten in Stahlschränken, den Zugangsregelungen zum Rechner zum Beispiel mittels PIN oder Token bis hin zum Zugriffsschutz durch explizite Freigabe von Berechtigungen. Des Weiteren ist die ordnungsgemäße Behandlung von nicht mehr benötigten Informationen und Datenträgern erforderlich. Hierzu sind entsprechende Lösch- und Vernichtungsgeräte zu verwenden.

Angriffsmöglichkeiten und IT-Sicherheit in ausgewählten Anwendungen und Technologien

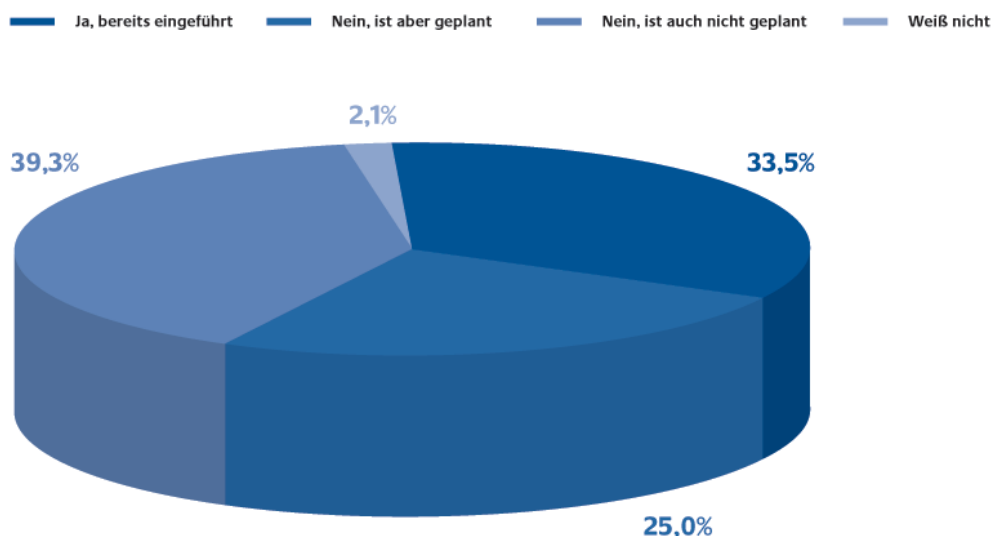


5 Angriffsmöglichkeiten und IT-Sicherheit in ausgewählten Anwendungen und Technologien

5.1 Voice over IP (VoIP)

Voice over IP (VoIP) gehört mittlerweile zum festen Bestandteil unserer Informations- und Kommunikationstechnik. Bei der Neukonzeption der Telekommunikationsinfrastruktur in der öffentlichen Verwaltung sowie in der Wirtschaft steht VoIP im Fokus.

Verbreitung von Voice over IP



Quelle: InformationWeek

Abbildung 6: Einsatz und geplante Einführung von Voice over IP in deutschen Unternehmen [7]

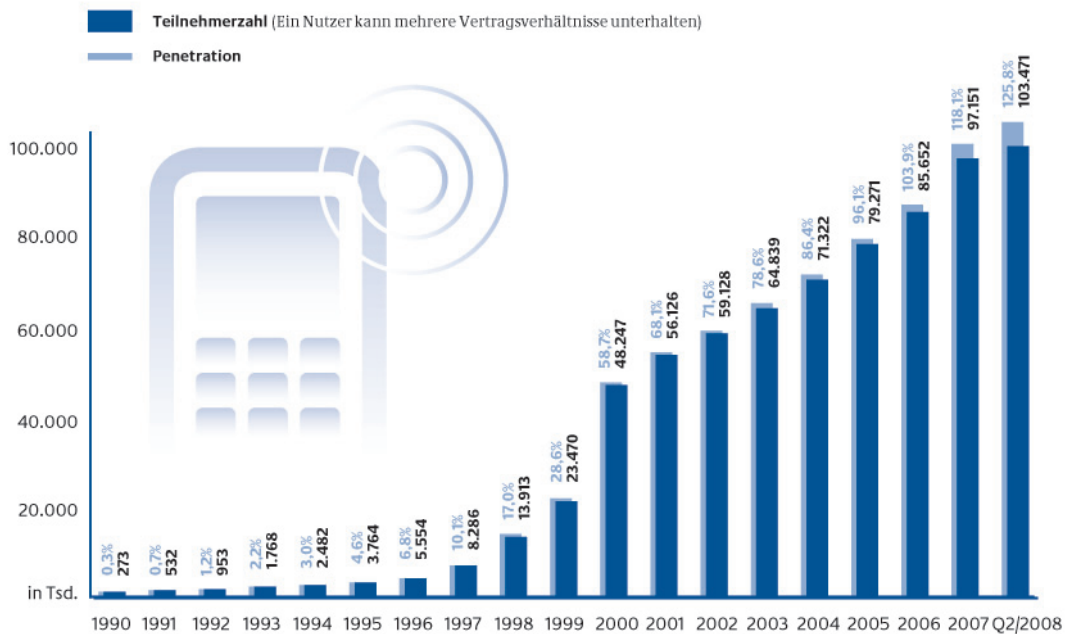
Auch Privatanwender greifen vermehrt auf diese Technologie zurück, da sie eine kostengünstige Alternative zur herkömmlichen Telekommunikation darstellt. Oftmals geschieht dies sogar unbemerkt, da Nutzer von ihren Telefon-, Internet- oder Kabelfernseh-Anbietern häufig eine zentrale, multifunktionale Box zur Verfügung gestellt bekommen. Über diese werden dann auch vorhandene Telefone angeschlossen und auf diese Weise VoIP genutzt. Für den Privatanwender ist dies nicht unbedingt ersichtlich.

Trotz der gestiegenen Verbreitung ist die Sicherheitslage von Voice over IP aus dem Blickwinkel der Informationssicherheit im Vergleich zum Jahr 2007 unverändert. Die seinerzeit aufgeführten Risiken wie Manipulation oder Ausfall bestehen weiterhin. Daher ist der Einsatz zusätzlicher Sicherungsmaßnahmen, wie zum Beispiel die Verschlüsselung der Signalisierungs- und Kommunikationsdaten in offenen Netzen oder die Verwendung einer für VoIP geeigneten Firewall, für den sicheren Betrieb von VoIP weiterhin erforderlich. Der Privat-anwender ist hier auf die Absicherung seitens der Anbieter angewiesen.

5.2 Mobile Kommunikation


Überall und zu jeder Zeit erreichbar sein: Endgeräte und Anwendungen mobiler Kommunikation sind heute für viele Unternehmen und Privatpersonen unverzichtbar. So liegt die Penetration in deutschen Mobilfunknetzen im Jahr 2008 bei über 120 Prozent der Gesamtbevölkerung. Dies zeigt, dass einige Nutzer sogar mehrere Vertragsverhältnisse unterhalten.[14]

Mobilfunk in Deutschland



Quelle: Bundesnetzagentur

Abbildung 7: Teilnehmerentwicklung und Penetration in deutschen Mobilfunknetzen [14]



Internetanwendungen wie E-Mail-Kommunikation, E-Commerce oder Online-Banking stehen zunehmend auch mobil zur Verfügung. Infrastrukturausbau und Nutzungsmotive werden sich hier auch künftig gegenseitig beeinflussen. In der Bundesrepublik wird mobile Kommunikation derzeit überwiegend über öffentliche Mobilfunknetze der zweiten und dritten Generation (GSM, UMTS) durchgeführt.

Mobile Endgeräte

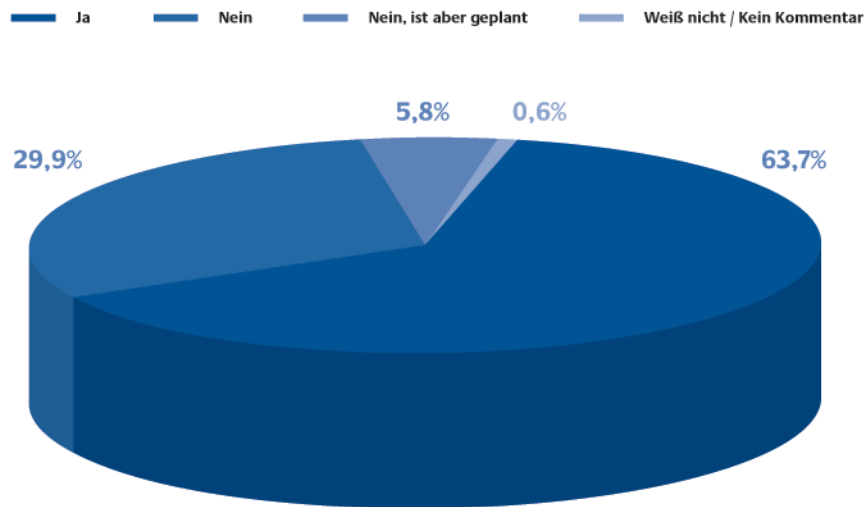
Die Verfügbarkeit mobiler breitbandiger Internetverbindungen wird in den kommenden Jahren weiter steigen und mit ihr die Verbreitung von Smartphones, PDAs und Subnotebooks. Dabei werden mobile Endgeräte in ihrer Softwareausstattung immer PC-ähnlicher. Aus diesem Grund und mit zunehmender mobiler Nutzung von Internet- und Datenkommunikationsdiensten steigt auch die Gefahr von Virus-Attacken und Angriffen mit Trojanischen Pferden stark an. Um den Bedrohungen wirkungsvoll zu begegnen, müssen geeignete Schutzmaßnahmen auf verschiedenen Ebenen – das heißt beim Netzbetreiber, auf den Übertragungstrecken, bei den mobilen Diensten und auf Seiten der mobilen Endgeräte – etabliert werden.

Aufgrund unterschiedlicher Interessenlagen werden zwar bereits auf allen Ebenen proprietäre Sicherheitslösungen eingesetzt. Allerdings sind diese zum Teil nicht öffentlich bekannt. Ein Gesamtkonzept für die IT-Sicherheit der Mobilkommunikations-Infrastruktur existiert bislang nicht.

WLAN, Bluetooth

Im lokalen sowie mobilen Bereich sind standardisierte Funkschnittstellen auf WLAN- und Bluetooth-Basis bereits weit verbreitet. Fast 60 Prozent der bundesdeutschen Haushalte sind bereits mit WLAN ausgestattet.[15] Bei den Unternehmen sind es noch etwas mehr.

WLAN-Verbreitung



Quelle: InformationWeek

Abbildung 8: Einsatz von Wireless LAN (WLAN) in deutschen Unternehmen [7]

Die Funkschnittstellen sind werkseitig auch heute noch häufig unsicher konfiguriert und stellen auf diese Weise ein zusätzliches IT-Sicherheitsrisiko dar. Derzeit werden in Deutschland immer noch unverschlüsselte oder schwach verschlüsselte (WEP) WLAN-Verbindungen betrieben. Dabei ist 83 Prozent der privaten WLAN-Nutzer bekannt, dass Dritte unter Umständen auf ihre Kosten surfen können.[6]

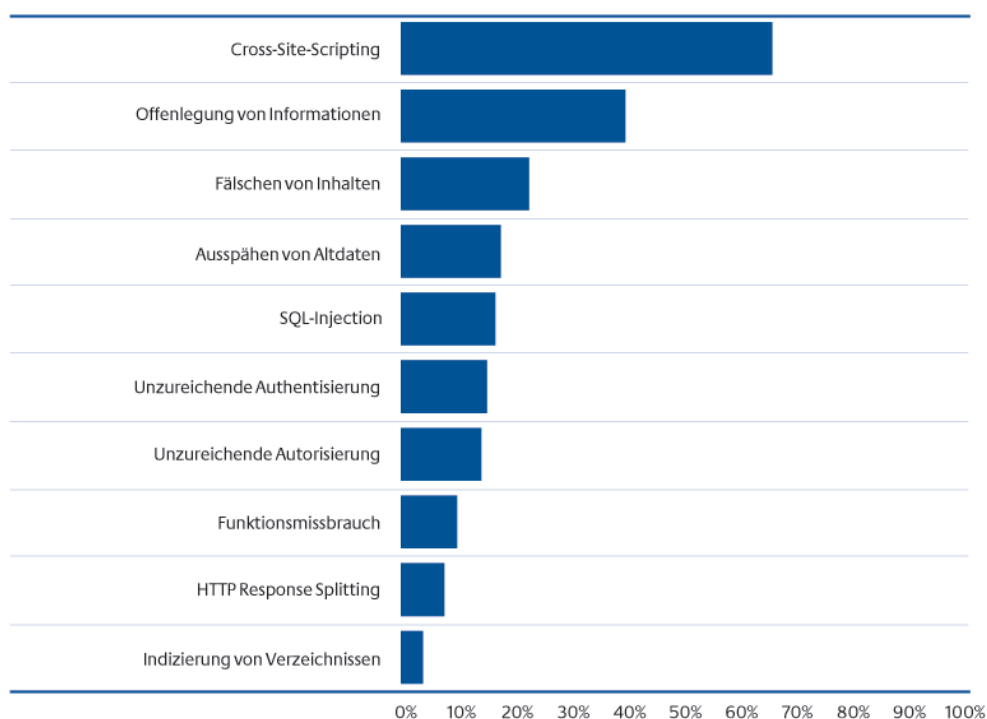
Für die kryptographische IT-Sicherheit der Bluetooth-Schnittstellen ist mit der schrittweisen Marktdurchdringung der Version 2.1 des Bluetooth-Standards Besserung zu erwarten. In dieser wurde das Sicherheitskonzept – unter anderem zur Verhinderung von Man-In-The-Middle-Attacken – überarbeitet und verbessert. Dennoch sollte grundsätzlich gelten, dass lokale Funkschnittstellen für Fremde möglichst unsichtbar und unzugänglich konfiguriert werden. Außerdem sollte die Schnittstelle zeitlich begrenzt, das heißt nur während der eigentlichen Nutzung, aktiviert werden.

5.3 Web 2.0

Die Anwendungen des Web 2.0 werden immer beliebter. Nutzer konsumieren nicht mehr nur die im Web verfügbaren Informationen, sondern bringen selbst Inhalte ein. Private Weblogs, Wikis, Social Networks, Bilder- und Video-Portale bieten auch Nutzern, die kein technisches Hintergrundwissen besitzen, die Möglichkeit, Inhalte im Internet zu publizieren. Laut einer Studie sind gut ein Drittel der Internetnutzer an der Option eigene Inhalte zu erstellen interessiert.[15]

Eine weit verbreitete Technik im Web 2.0 ist AJAX (Asynchronous JavaScript and XML). Mithilfe dieser Technik können einzelne Teile einer Webseite nachgeladen werden, ohne dass dabei die komplette Seite übertragen werden muss. Auf diese Weise lassen sich Desktop-ähnliche Webangebote realisieren. Dazu muss der Browser des Nutzers jedoch für Aktive Inhalte freigeschaltet sein. Bereits im Lagebericht 2007 wurde darauf hingewiesen, dass dies unter Sicherheitsaspekten kritisch zu bewerten ist, da hierbei Programmcode an den Client übertragen wird. Schafft es ein Angreifer seinen eigenen Code in eine Webseite einzuschleusen, so kann er auf dem Client, der diese Webseite besucht, prinzipiell beliebigen Code ausführen. Um dies zu erreichen, muss ein Angreifer eine Webseite finden, die entsprechende Schwachstellen aufweist. Die Wahrscheinlichkeit dafür ist recht hoch. Laut einer Studie weisen 90 Prozent aller Webseiten Schwachstellen auf. Den Großteil machen dabei Schwachstellen aus, die Cross-Site-Scripting-Angriffe erlauben. Cross-Site-Scripting (XSS) ermöglicht einem Angreifer unter anderem Inhalte von Webseiten zu verändern oder Benutzer-Sessions zu übernehmen. Etwa 65 Prozent aller Webseiten sind für diese Art von Angriff anfällig.[16]

Schwachstellen in Webseiten



Quelle: WhiteHat

Abbildung 9: Wahrscheinlichkeiten für das Vorhandensein bestimmter Schwachstellen [16]

Gelingt einem Angreifer das Einschleusen von schädlichem Programmcode, kann er beispielsweise eine bestehende Sitzung bei einem Online-Shop übernehmen. Somit ist er in der Lage, Tastatureingaben wie Benutzernamen und Passwörter aufzuzeichnen oder mittels Schwachstellen im Webbrowser das ganze System des Nutzers unter seine Kontrolle zu bringen.

Als wirksame Schutzmaßnahme hat sich bisher nur das Deaktivieren sämtlicher Aktiver Inhalte im Browser des Nutzers erwiesen. Mit zunehmendem Wunsch der Anwender, Webangebote aktiv mitzugestalten, schwindet jedoch gleichzeitig deren Bereitschaft, auf Aktive Inhalte zu verzichten. Denn dies hat zur Folge, dass sich Webangebote, die bestimmte Technologien verwenden, nicht mehr anzeigen lassen. Für einige Webbrowser existieren zusätzliche Plug-Ins, die es erlauben, die Restriktionen bezüglich Aktiver Inhalte graduierter zu steuern. Aber auch diese Plug-Ins bieten keinen absoluten Schutz. Zudem muss der Benutzer bei der Verwendung dieser Plug-Ins selbst entscheiden, ob eine Webseite vertrauenswürdig ist oder nicht.

5.4 Prozesssteuerungssysteme – SCADA

Kritische Infrastrukturen wie beispielsweise die Telekommunikation, das Transportwesen oder auch die Stromversorgung müssen möglichst ohne gravierende Unterbrechungen arbeiten, da das Wohl der Gesellschaft stark von ihrer Verfügbarkeit abhängt. Zur Bereitstellung der zugehörigen Dienstleistungen werden oftmals Prozesssteuerungs- bzw. SCADA (Supervisory Control and Data Acquisition)-Systeme eingesetzt. Aus organisatorischen und ökonomischen Gründen werden diese Systeme zunehmend untereinander oder mit anderen Netzen verbunden, was neue sicherheitstechnische Herausforderungen mit sich bringt.

Sollte ein Angreifer – zum Beispiel indirekt über das Bürokommunikationsnetz eines Betreibers – Zugriff auf Prozesssteuerungssysteme erlangen, könnte er die vom Internet bekannten Angriffsmethoden nutzen, um die Systeme zu stören. Das Gefahrenpotenzial ist besonders hoch, da schon kurze Störungen, wie beispielsweise der Neustart eines Systems, einen Produktionsprozess empfindlich beeinträchtigen können. Auch sind aufgrund der hohen Verfügbarkeitsanforderungen einige Standard-Sicherheitsmaßnahmen wie der Einsatz und die regelmäßige Aktualisierung von Anti-Virenprogrammen bei Produktionssystemen nicht ohne weiteres anwendbar.

Sowohl die Hersteller als auch die Nutzer von Prozesssteuerungssystemen werden sich der Gefährdungssituation zunehmend bewusst. Die besonderen Sicherheitsanforderungen von Produktionssystemen werden nach und nach in Empfehlungen und Standards berücksichtigt (vgl. Kapitel 3.2).

Dennoch sind die heute vertriebenen und eingesetzten Prozesssteuerungssysteme oftmals noch nicht ausreichend geschützt. So wurden auch 2008 verschiedene Schwachstellen aufgedeckt, zwei davon in weit verbreiteten Softwareprodukten zur Kontrolle von SCADA-Systemen. Wegen einer fehlerhaften Systemarchitektur führte in den USA ein Softwareupdate in einem Kernkraftwerk zu einem ungeplanten 48-stündigen Ausfall des Werks, weil das Prozesssteuerungssystem durch das Softwareupdate im Bürokommunikationsnetz gestört wurde. Vergleichbare Fälle in Deutschland sind nicht bekannt. Um Prozesssteuerungssysteme zu schützen, müssen speziell auf die Produktionsumgebung angepasste Sicherheitskonzepte entwickelt und umgesetzt werden. Einzelne, speziell auf Produktionssysteme ausgerichtete IT-Sicherheitsprodukte sind bereits am Markt verfügbar.

Da die Abhängigkeit unserer Gesellschaft von Kritischen Infrastrukturen, die von Prozesssteuerungs- bzw. SCADA-Systemen gesteuert werden, weiter zunimmt, muss das Ziel einer sicheren Gestaltung dieser Systeme intensiv weiterverfolgt werden.

5.5 Internetdienst: Domain Name System (DNS)

Zur Nutzung des Internets stehen dem Anwender verschiedene Dienste wie beispielsweise E-Mail oder das World Wide Web (WWW) zur Verfügung. Eine grundlegende Basis für die Funktion vieler Internetdienste stellt der für die Namensauflösung zuständige DNS (Domain Name System)-Dienst dar. Im Internet gebräuchliche Hostnamen wie `www.bsi.bund.de` werden mit Hilfe des Domain Name Systems in IP-Adressen umgewandelt (im Beispiel `77.87.228.49`). So muss der Nutzer in der Regel IP-Adressen nicht direkt verwenden. Die Integration der Hostnamen bzw. des DNS in nahezu alle gebräuchlichen Internetdienste macht das Domain Name System zu einem der wichtigsten Dienste im Internet.

Das bei einer Kommunikation zwischen den einzelnen DNS-Servern zum Datenaustausch verwendete Kommunikationsprotokoll weist konzeptionelle Schwachstellen auf und ist unzureichend vor Manipulationen durch Dritte geschützt. Eine sehr ernst zu nehmende Schwachstelle wurde zuletzt im Juli 2008 bekannt. Angreifer hatten die Möglichkeit, den Internetverkehr umzulenken, Daten mitzulesen und Inhalte zu manipulieren. Bis alle Provider mit entsprechenden Updates reagiert hatten, waren Millionen Nutzer für mehrere Tage einem hohen Manipulationsrisiko ausgesetzt.

In der Vergangenheit wurden einige Maßnahmen, die solche Angriffe erschweren sollen, jedoch nicht verhindern können, durch die Betreiber umgesetzt. Zur generellen Verbesserung der Sicherheit des Domain Name Systems wurde in der Fachwelt eine Erweiterung des zugrunde liegenden Protokolls mit dem Namen DNSSEC entwickelt. Dabei stellen kryptographische Verfahren die Authentifizierung und Datenintegrität der DNS-Daten sicher.

Einige Betreiber von Top-Level-Domains (die höchste Ebene der Namensauflösung) haben diese Erweiterung zwischenzeitlich eingeführt. In der EU signiert Schweden seit 2005 die Top-Level-Domain `.se`. Der Betreiber der Top-Level-Domain `.org` plant die Einführung bis 2010. Bisher scheiterte eine globale Einführung jedoch an den dazu notwendigen Änderungen in der Infrastruktur und den Arbeitsabläufen.

5.6 Multifunktionsgeräte

Multifunktionsgeräte sind eine platzsparende und kostengünstige Lösung, um die Funktionen Scannen, Drucken, Kopieren und oft auch Faxen zur Verfügung zu stellen. Aus diesem Grund werden sie zunehmend eingesetzt. Es existieren sowohl netzfähige Geräte, die einer größeren Benutzergruppe zur Verfügung stehen, als auch Einzelplatzlösungen, beispielsweise mit einer USB-Schnittstelle.

Durch die Integration der Funktionen Scannen, Drucken und Kopieren in einem Gerät steigen die IT-Sicherheitsanforderungen im Vergleich zu einzelnen Systemen, da solche Geräte zusätzlich einen so genannten Single Point of Failure darstellen. Dies bedeutet, dass beim Ausfall einer Funktionalität das gesamte Gerät repariert werden muss, so dass auch die nicht betroffenen Dienste während dieser Zeit nicht mehr genutzt werden können.

Werden Informationen, wie beispielsweise eingescannte Dokumente, im Speicher abgelegt, können unter Umständen auch unberechtigte Personen darauf zugreifen. Im einfachsten Fall ist es dabei lediglich möglich, das zuletzt gespeicherte Dokument auszudrucken. Problematischer ist es, wenn Angreifer den gesamten Speicher auslesen können, um dessen Inhalt zu analysieren. Manche Hersteller sind zur Statistikerstellung und zu Wartungszwecken dazu übergegangen, Daten direkt vom Kundendrucker an einen eigenen Server zu senden. Oft ist nicht dokumentiert oder nachprüfbar, welche Daten dabei an den Hersteller übermittelt werden.

Neben dem ungewollten Informationsfluss aus dem LAN heraus könnte ein netzfähiger Drucker auch unerwünscht Daten aus dem Internet empfangen und eventuell weiterverteilen. Ein Beispiel ist Schadsoftware, die nicht nur das Gerät in seiner Funktion beschränkt, sondern weitere IT-Systeme im Netz infiziert. Schadsoftware könnte beispielsweise durch manipulierte Patches aus dem Internet eingespielt werden. Ein Netzdrucker kann dadurch unter Umständen zu einem Einfallstor für Angriffe aus dem Internet werden.

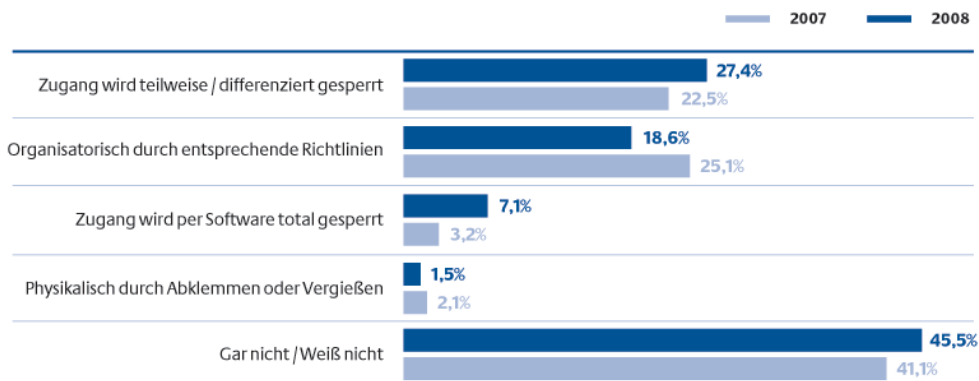
5.7 Schnittstellen und Speichermedien

Externe Speichermedien zum einfachen Austausch und Transport großer Datenmengen gewinnen immer mehr an Bedeutung. Als Schnittstellen für einen Datenaustausch mit externen Speichermedien haben sich Firewire und USB (Universal Serial Bus) etabliert. Die Schnittstellen bieten aber auch eine zusätzliche Möglichkeit, um Schadsoftware auf Rechner zu schleusen. Während USB nur einen passiven Zugriff auf den PC erlaubt, ist es über die Firewire-Schnittstelle prinzipiell möglich, auch aktiv mit dem PC zu kommunizieren. Damit kann bei einer aktiven oder von außen aktivierbaren Firewire-Schnittstelle vom Betriebssystem unbemerkt auf den Speicher des Rechners zugegriffen werden. So können Passwörter oder Schlüssel von aktiven Kryptoverfahren ausgelesen werden. Der Einsatz eines aktuellen Virens scanners und das Deaktivieren nicht benötigter Schnittstellen kann das Gefahrenpotenzial reduzieren.

Für den einfachen Datenaustausch werden vorwiegend USB-Sticks verwendet. Allein in einem Jahr wurden über 85 Millionen dieser Datenträger verkauft.[17] Auf etwa 80 bis 90 Prozent der USB-Sticks werden die Daten immer noch unverschlüsselt transportiert. Viele Hersteller gehen dazu über, Schutzmechanismen direkt in die Sticks zu implementieren. Für die eigentliche Sicherheitssoftware besteht aber trotzdem ein Manipulationsrisiko, da sie nicht im geschützten Bereich liegen kann. Schutzmechanismen, die keine Verschlüsselung beinhalten, können durch direktes Auslesen des Flash-Speichers umgangen werden. Für andere Speichermedien wie zum Beispiel SD-, MMC- oder CF-Speicherkarten ergibt sich die gleiche Problematik. Ein einfacher Schreibschutzschalter kann die Daten auf einem externen Medium wirkungsvoll vor Manipulationen schützen. Beim Einbringen in ein Fremdsystem lassen sich so die Daten nicht unbemerkt verändern. Jedoch bieten gerade bei den USB-Sticks immer weniger Hardwarehersteller einen mechanischen Schreibschutzschalter an.

Die Anzahl externer Speichermedien wird in Zukunft weiter zunehmen. Trotzdem wird auf die Gefahren, die von diesen Speichermedien und den offenen Schnittstellen ausgehen, noch immer nicht ausreichend reagiert. Laut einer Umfrage im Jahr 2008 sichern 45,5 Prozent der Unternehmen ihre Schnittstellen nicht ab bzw. können keine Angaben dazu machen.[7] Im Vergleich zum Vorjahr ist hier sogar ein Zuwachs zu verzeichnen. So besteht weiterhin ein hohes Gefahrenpotenzial durch gezielte Angriffe auf externe Speichermedien und Schnittstellen.

Absicherung von Schnittstellen



Quelle: InformationWeek

Abbildung 10: Absicherung von Peripherie-Schnittstellen (zum Beispiel USB) in deutschen Unternehmen [7]

5.8 Netzkoppelemente

Durch die zunehmende Vernetzung von IT-Systemen sind Netzkoppelemente (Geräte wie Router und Switches) aus Internet und Intranet nicht mehr wegzudenken. In Unternehmen und Behörden nehmen Netzkoppelemente zunächst ihre ursprüngliche Aufgabe wahr: die Steuerung des Netzwerkverkehrs. Zusätzliche Aufgaben können in der Segmentierung eines Netzwerkes, der Filterung von Netzwerk-Paketen, der Umsetzung von Netzwerk-Adressen (Network Address Translation, kurz NAT) oder der Anbindung von Speichernetzwerken bestehen. Den steigenden Anforderungen, wie etwa der Priorisierung von Netzwerkverkehr oder der Erkennung und Abwehr von Angriffen und Schadprogrammen, begegnen die Hersteller mit einer größeren Funktionsvielfalt der Produkte. Doch nicht nur im professionellen Bereich kommen Netzkoppelemente zum Einsatz. Mit der zunehmenden Verbreitung von Breitband-Internetzugängen haben Router auch in vielen Privathaushalten Einzug gehalten.

Die Verfügbarkeit und Integrität von Netzkoppelementen ist für Unternehmen und Behörden gleichermaßen bedeutsam. Zusätzlich ist die Vertraulichkeit der Daten, die über die Netzwerkgeräte ausgetauscht werden, zu gewährleisten. Für einen Angreifer stellen solche Knotenpunkte strategische Ziele dar. Es kann nicht nur ein einzelner Rechner angegriffen werden, sondern die Kommunikation aller IT-Systeme, die mit dem Netzwerkgerät verbunden sind, manipuliert werden. Auch in Privathaushalten sind Netzkoppelemente ein mögliches Angriffsziel.


Angriffe auf Netzkoppelemente sind eine ernst zu nehmende Gefahr. Die Anzahl der gemeldeten Schwachstellen in Netzkoppelementen ist im ersten Halbjahr 2008 im Vergleich zum Vorjahreszeitraum um 61 Prozent gestiegen.[18]

Die Gefahr eines Angriffs kann reduziert werden, indem aktuelle und um Schwachstellen bereinigte Betriebssystem- bzw. Firmware-Versionen eingesetzt werden. In Kombination mit sicheren Authentifizierungsmechanismen, der regelmäßigen Auswertung der Protokolldaten von Netzwerkgeräten sowie der Sicherstellung der Betriebssystem- bzw. Firmware-Integrität kann einem Angriff auf Netzkoppelemente vorgebeugt werden.

5.9 Service-orientierte Architekturen (SOA)

Die Architektur moderner IT-Systeme orientiert sich immer stärker an den Geschäftsprozessen, die diese Systeme unterstützen. Service-orientierte Architekturen (SOA) beschreiben einen allgemeinen Ansatz zur Realisierung komplexer IT-Systeme und der Abbildung von Geschäftsprozessen in solchen Systemen. Aufgrund ihrer geschäftsprozessnahen Ausrichtung sind SOA gerade für Managementkreise besonders interessant, da der Übergang zwischen Geschäftsleitung und IT fließend ist. Dies führt insbesondere zu schnelleren und kostengünstigeren Anpassungen bei Änderungen der Geschäftsprozesse. Auch die Integration und Interaktion unterschiedlicher Teilsysteme gestalten sich in einer Service-orientierten Architektur deutlich einfacher. Daher ist der SOA-Ansatz schon heute weit verbreitet und wird in Zukunft noch stärker in den Mittelpunkt rücken.

Da die verschiedenen Dienste in einer SOA über Unternehmensgrenzen hinweg verteilt sein können, sind nicht mehr alle beteiligten Dienste und Ressourcen unter der eigenen Kontrolle, sondern befinden sich in fremden Domänen. Die Sicherheitsanforderungen an SOA-Infrastrukturen sind aufgrund der darin stattfindenden vertraulichen Geschäftstransaktionen daher hoch. Neben der Problematik verteilter Strukturen, realisiert durch offene Formate, betrifft dies auch Administrations- und Beherrschbarkeitsaspekte. Die Realisierung eines Geschäftsprozesses über eine Vielzahl lose gekoppelter Services erfordert beispielsweise mehr Authentisierungsvorgänge und eine höhere Integrität als konventionelle Systeme. Außerdem muss jederzeit Vertraulichkeit gewährleistet sein.



Viele der potenziellen Risiken konventioneller Systeme finden sich auch in SOA wieder. Bekannte Bedrohungen, wie beispielsweise das Einschleusen von Schadcode, sind hier ebenfalls möglich, jedoch über andere Wege und Methoden. Durch die homogene, systemübergreifende Architektur von SOA kann die Ausbreitung von Schadcode begünstigt werden. Zusätzlich ergeben sich neue Angriffsmöglichkeiten wie zum Beispiel potenzielle Schwachstellen von XML-Signaturen oder schwache Implementierungen SOA-spezifischer Standards und Technologien.

SOA kann dann wirklich revolutionär sein, wenn das sicherheitsspezifische Potenzial in seiner vollen Breite ausgeschöpft wird. Eine Vielfalt an offenen Technologien und Standards ist – insbesondere im Sicherheitsbereich – schon heute verfügbar und in vielen Produkten bereits implementiert.

Chancen und Risiken innovativer Anwendungen und Technologien



6 Chancen und Risiken innovativer Anwendungen und Technologien

Innovation schafft Zukunft und eröffnet Chancen. Wettbewerbsvorteile können realisiert werden. Oft beinhalten technische Innovationen aber auch sicherheitsspezifische Herausforderungen. Interessen und Anforderungen von Herstellern und Anwendern gehen mitunter auseinander. Um sich langfristig am Markt durchzusetzen, muss eine Technologie im Hinblick auf Sicherheit jedoch bestimmten Standards entsprechen.

6.1 Radio Frequency Identification (RFID)

Die RFID-Technik ist eine für viele Anwendungen nutzbringende Technologie. Daher hat sich ihr Einsatz in den vergangenen Jahren stetig ausgeweitet. Populäre Beispiele hierfür sind alle Arten von Ticketing-Systemen – von der Eintrittskarte für ein Fußballspiel bis hin zum Jahresticket für den öffentlichen Nahverkehr. Der Einsatz der RFID-Technik führt zu erhöhter Fälschungssicherheit und optimierten Kontrollprozessen.

Wie nahezu jede innovative Technologie hat auch der RFID-Einsatz mit Akzeptanzproblemen zu kämpfen. Die Angst, dass Daten von unautorisierten Dritten ausgelesen oder verändert werden könnten, lässt Endnutzer der Technologie skeptisch gegenüberstehen.

Seit Erscheinen des Lageberichts 2007 wurde mit den wachsenden Einsatzmöglichkeiten auch dem Thema Sicherheit ein größerer Stellenwert eingeräumt. So entwickelte das BSI mithilfe von Industrie, Verbraucherschutzverbänden und den Datenschutzkontrollbehörden Technische Richtlinien. Diese geben detaillierte Maßnahmen für den sicheren Einsatz der RFID-Technologie in verschiedenen Gebieten vor und können als Leitlinie für einen sicheren RFID-Einsatz verstanden werden.


Mithilfe solcher Richtlinien ist es möglich, dem Anwender der RFID-Technik ein bestimmtes Sicherheitsniveau zu garantieren. So erhalten zum Beispiel implementierte Sicherheitsmaßnahmen nach erfolgreicher Prüfung ein Zertifikat durch einen unabhängigen Prüfer.

Auch von dem europäischen Datenschutzbeauftragten wurde die Technische Richtlinie als gutes Beispiel hervorgehoben. Das BSI hofft durch die Teilnahme an der Konsultation der europäischen Kommission zu den Sicherheits- und Datenschutzaspekten des RFID-Einsatzes einer europäischen Anerkennung der Richtlinienwerke ein Stück näher gekommen zu sein.

6.2 Biometrie, Personaldokumente und Bürgerservices

Durch die eCard-Strategie der Bundesregierung werden die Kartenprojekte der Bundesverwaltung – die elektronische Gesundheitskarte (eGK), der elektronische Personalausweis, der elektronische Einkommensnachweis (ELENA) und die elektronische Steuererklärung (ELSTER) – eng aufeinander abgestimmt. Gleiche Standards und die breite Verwendbarkeit der Chipkarten für den elektronischen Geschäftsverkehr sollen Effizienzgewinne und Kosteneinsparungen zum Nutzen von Bürgerinnen und Bürgern, Wirtschaft und Verwaltung gewährleisten. Mittels des vom BSI entwickelten „eCard-API-Framework“, einer technischen Spezifikation, die einen einfachen und einheitlichen Zugriff auf die Funktionen unterschiedlicher Chipkarten ermöglicht, wird die eCard-Strategie der Bundesregierung in technischer Hinsicht und bezüglich der Sicherheit der Daten auf ein solides Fundament gestellt.

Neben der eCard-Strategie der Bundesregierung wird auch die Ausstattung hoheitlicher Dokumente mit biometrischen Merkmalen weiter verfolgt. Nach der Einführung der zweiten Stufe des elektronischen Reisepasses (ePass) wird auch der zukünftige Personalausweis biometrische Daten tragen. Damit kann die Bindung des Inhabers an das Dokument deutlich gesteigert und Missbrauch vermieden werden. Um den sicherheitstechnischen Herausforderungen zu begegnen, werden die technischen Standards zu Datenschutz und Datensicherheit maßgeblich vom BSI mitgestaltet, so dass unberechtigte Zugriffe auf die in den Dokumenten gespeicherten Daten verhindert werden können.



Als innovative Zukunftstechnik wird Biometrie jedoch auch jenseits von hoheitlichen Dokumenten zunehmend eingesetzt. Im privatwirtschaftlichen Bereich reicht der Einsatz von Biometrie-basierten Zugangskontrolllösungen bis zu Biometrie-gestützten Zahlungssystemen. Bei der Auswahl biometrischer Systeme sollten daher immer die benötigten Sicherheits- bzw. Komfortniveaus im Fokus stehen. Die Definition einheitlicher Sicherheitsstufen für biometrische Verfahren wird daher eine wichtige Aufgabe in den kommenden Jahren sein.

Getrennt von der Aufnahme biometrischer Merkmale, bietet der im elektronischen Personalausweis integrierte Chip auch die Option, das Dokument um eine Funktion zu erweitern, die dem Inhaber ermöglicht, seine Identität auch über unsichere Netze wie dem Internet nachweisen zu können (eID-Funktion). Durch ein Berechtigungskonzept wird sichergestellt, dass nur befugte Stellen auf den Ausweis zugreifen können. Der Inhaber muss sämtliche Zugriffe durch PIN-Eingabe explizit genehmigen. Insgesamt steht dem Anwender eine neue IT-Infrastruktur zur Verfügung, mit der Anwendungen im E-Government, E-Business und E-Commerce einfach und vertrauenswürdiger genutzt werden können. Eine zusätzliche Anwendung des elektronischen Personalausweises ist eine Signaturanwendung, wie sie bereits heute auf separaten Signaturkarten zu finden ist.

Ein Dienst, bei dem die eID-Funktion dieses Internetausweises zum Einsatz kommen soll, ist die Anmeldung des Karteninhabers an seinem Bürgerportalkonto. Im Projekt „Bürgerportale“ wird unter Federführung des Bundesministeriums des Innern (BMI) ein Konzept zur sicheren und vertraulichen Kommunikation im Internet zusammen mit der Wirtschaft unter dem Namen „De-Mail“ erarbeitet. Ein Verbund privater, aber staatlich zertifizierter Anbieter soll eine Infrastruktur liefern, so dass E-Mails zuverlässig und geschützt versendet werden können. Eine sichere Dokumentenablage basierend auf dem sicheren Identitätsnachweis mit dem elektronischen Personalausweis ergänzt das Konzept.

Durch die gesteigerte Nutzung der eID-Funktion des elektronischen Personalausweises im privatwirtschaftlichen Umfeld ist davon auszugehen, dass in Zukunft verstärkt Angriffe auf die betreffenden Sicherheitsfunktionen stattfinden werden.

6.3 IPv6

Für die Übertragung der Daten im Internet ist das Internet Protokoll (IP) zuständig. Ein wesentlicher Bestandteil dieses Protokolls sind die IP-Adressen. Analog zu den Adressen auf einem Briefumschlag werden die IP-Adressen benötigt, damit Internet Service Provider (ISP) die Datenpakete an die Empfänger bzw. die Internetnutzer ausliefern können.

Heute wird überwiegend das Internet Protokoll in der Version 4 (IPv4) eingesetzt. Die zugehörigen IP-Adressen bestehen aus 4 Bytes (also 32 Bit). Insgesamt sind somit 4.294.967.296 IP-Adressen möglich.

Mit zunehmendem Wachstum des Internets werden immer mehr IP-Adressen verbraucht. Heute geht man davon aus, dass die Vergabestellen etwa ab dem Jahr 2012 keine neuen IPv4-Adressen mehr verteilen können. Ein Wachstum des Internets wäre ab dann nicht mehr wie bisher möglich. Bereits vor einigen Jahren wurde daher mit den Arbeiten an einer neuen IP-Version begonnen und das IP-Protokoll in Version 6 (IPv6) standardisiert. Die neuen zugehörigen IP-Adressen haben eine Länge von 128 Bit. Demnach gibt es somit 340.282.366.920.938.463.463.374.607.431.768.211.456 (ca. 340 Sextillionen) IP-Adressen. Damit stehen für lange Zeit genügend IP-Adressen zur Verfügung.

IPv6 ist bei vielen Internet Service Providern bereits getestet. Trotzdem zögern sie wegen des hohen Realisierungsaufwands und der geringen Kundennachfrage mit der Einführung. Die rechtzeitige Einführung von IPv6 ist jedoch zwingend notwendig, um das Wachstum des Internets auf lange Sicht nicht zu bremsen.

Künftig werden sich aus der Verwendung des neuen Protokolls auch neue Herausforderungen für die Sicherheit ergeben. Diese gilt es sorgfältig zu bestimmen. Wirkungsvolle Gegenmaßnahmen müssen bereits bei der Realisierung berücksichtigt werden. Vor der Einführung sind umfangreiche Tests notwendig, um für einen reibungslosen Ablauf zu sorgen. Außerdem ist neben dem Betrieb der für IPv6 zuständigen Komponenten noch über Jahre hinweg der Parallelbetrieb für die IPv4-Komponenten einzuplanen.

6.4 IT-Sicherheit in Automobil und Verkehr

Fahrerassistenzsysteme

In keinem öffentlichen Bereich ist eine solche Zunahme von vernetzten informationstechnischen Komponenten zu beobachten wie im automobilen Umfeld. Elektronische Steuergeräte sowie hard- und softwarebasierte Computer sind mittlerweile zentraler Bestandteil moderner Fahrzeuge. Sie steuern praktisch alle Funktionen, die noch vor kurzem von elektromechanischen Komponenten übernommen wurden. Aufgrund ihrer Eigenschaften (softwarebasiert, vernetzt und hoch integriert) bieten sie flexible Ansätze für die Realisierung von Fahrerassistenzsystemen, wie zum Beispiel Spurhalteassistent, Abstandsregeltempomat und Vierradlenkung.

Derartige Funktionen sind jedoch auf ein verlässliches Echtzeit-Datennetzwerk mit höchster Verfügbarkeit angewiesen, das zudem wirksam gegen Manipulation geschützt sein muss. Ein Fahrzeug verfügt über bis zu 150 Steuergeräte, die über zahlreiche vernetzte Systeme Anwendungsdaten mit unterschiedlichen (Echtzeit)-Anforderungen austauschen. Dies stellt für die IT-Sicherheit eine in ihrer Gesamtheit nur schwer zu überblickende Herausforderung dar. Aus diesem Grund sind integrative Sicherheitskonzepte sowie herstellerübergreifende Standards und Empfehlungen für alle Phasen des Entwurfs, des Baus und der Nutzung von Fahrzeugen erforderlich. Bedrohungen wie Schadprogramme oder böswillige Manipulationen von Betriebssystemen stellen im automobilen Umfeld eine für die Risikobetrachtung ganz neue Größenordnung dar. Hier sind schließlich nicht nur wirtschaftliche Werte, sondern letztendlich Menschenleben zu schützen.

Das automobiler Netz


Künftig sollen Entwicklungen im Bereich der Kommunikation zwischen Fahrzeugen oder mit der Verkehrsinfrastruktur dazu beitragen, den Verkehrsfluss zu optimieren und die Unfallzahlen zu senken. Erreicht werden soll dies zum Beispiel durch gegenseitige Warnungen der Fahrzeuge untereinander (Car-to-Car) oder Warnungen von Sendestationen entlang der Straße (Infrastructure-to-Car) vor Gefahren wie einem Stauende oder Glatteis.

Hier bestehen besondere Herausforderungen in der Sicherstellung von Integrität und Authentizität der übermittelten Nachrichten unter Echtzeitbedingungen bei gleichzeitiger Berücksichtigung des Datenschutzes. Fälschungen müssen verhindert oder zweifelsfrei als solche erkannt und verworfen werden können, wobei die Anonymität der Nutzer nicht unangemessen beeinträchtigt werden darf. Aber auch gegen böswilliges Stören von Diensten mit dem Ziel, ihre Nutzbarkeit einzuschränken oder unmöglich zu machen (DoS-Angriffe), müssen Maßnahmen getroffen werden. Hier wird langfristig eine neue und anspruchsvolle Kommunikationsinfrastruktur mit Verbindungen zu den bestehenden Daten- und Kommunikationsnetzen zu errichten sein. Diese muss ihrer volkswirtschaftlichen Bedeutung hinsichtlich der IT-Sicherheit und den damit verbundenen Risiken gerecht werden.

6.5 Elektronische Gesundheitskarte (eGK)

Mit der Einführung der elektronischen Gesundheitskarte wird in Deutschland ein bundesweites Gesundheitsnetzwerk geschaffen. Die Digitalisierung der medizinischen Versorgung gehört zu den anspruchsvollsten IT-Projekten weltweit. Experten rechnen mit über zehn Milliarden Datentransaktionen pro Jahr und schätzen das Datenaufkommen auf mehrere Dutzend Terabyte.

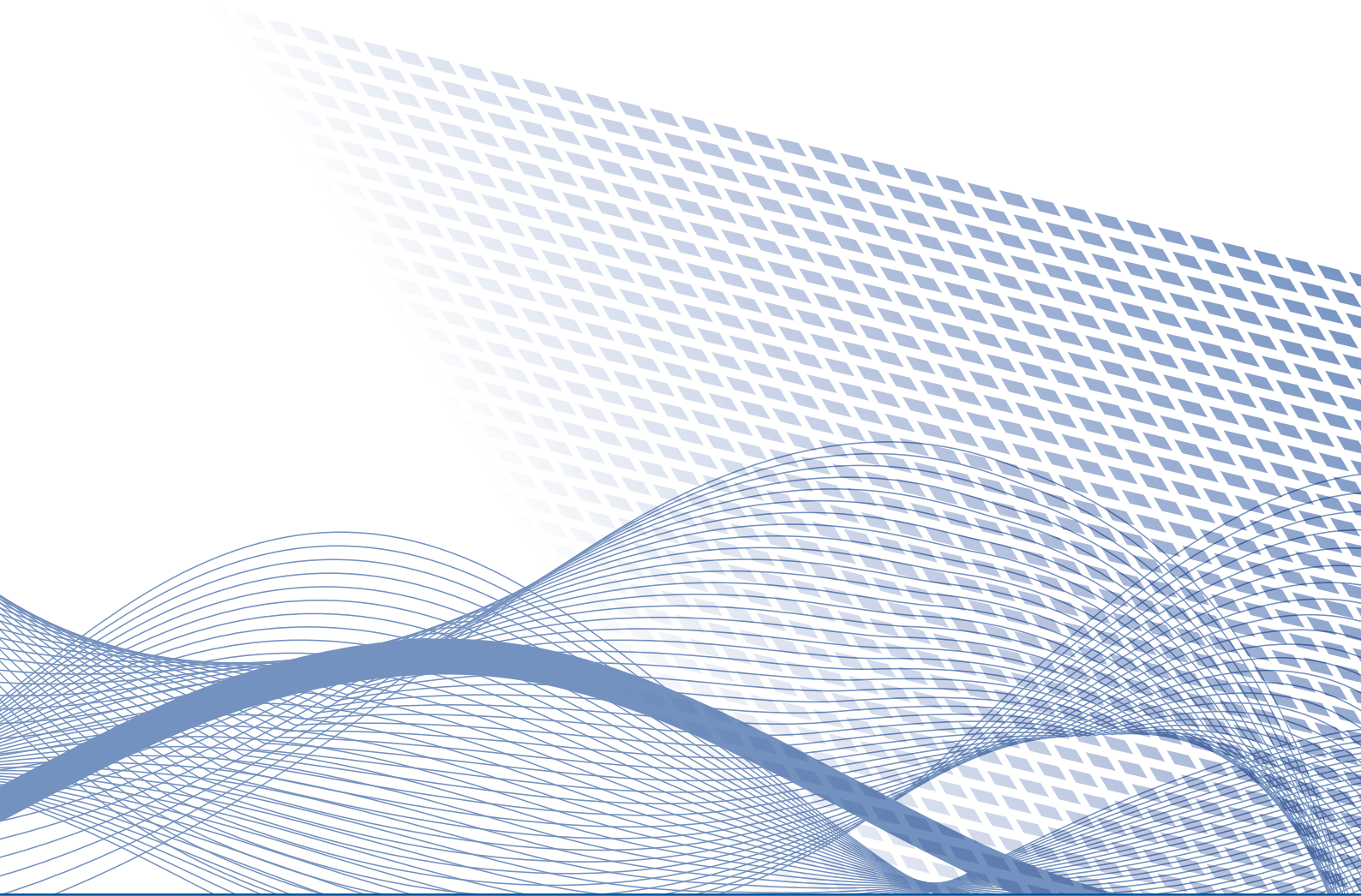
Die Technologie kontaktbasierter Chipkarten ist nicht neu. Die erstmalige Anwendung auf derart breiter Basis stellt jedoch in großem Maße neue Anforderungen an die Sicherheit, vor allem in den Bereichen der IT-Infrastruktur und des Datenschutzes. So darf die Vernetzung nicht dazu führen, dass durch kriminelle Angriffe, technische Schwachstellen oder menschliche Fehler Informationen über die Krankheiten des Karteninhabers von Unbefugten gelesen werden können. Auch die ständig wachsende Anzahl allgemeiner Bedrohungen in der Informationstechnik – etwa ausspionierte Passwörter, Trojanische Pferde oder manipulierte Sicherheitssysteme – können die Vertraulichkeit der Informationen, die Arzt und Patient austauschen, gefährden.



Die Verschlüsselung der Daten spielt daher eine entscheidende Rolle. Sie ermöglicht eine sichere Zugriffs- und Rechteverwaltung. Ziel ist es, vertrauliche Informationen in ein eigenes Gesundheitsnetzwerk, der so genannten Telematikinfrastruktur, innerhalb des weltweiten Datennetzes zu verschicken.

Das BSI unterstützt das Bundesministerium für Gesundheit (BMG) bei der Einführung der elektronischen Gesundheitskarte in Fragen der IT-Sicherheit. Es beteiligt sich aktiv an der Entwicklung funktionaler Spezifikationen verschiedener Komponenten wie zum Beispiel der Gesundheitskarte selbst, dem Heilberufausweis sowie Kartenterminals und Konnektoren. Des Weiteren entwickelt das BSI Prüfvorschriften für diese Produkte. Die Sicherheitszertifizierung des BSI auf Basis dieser Prüfvorschriften ist zentraler Bestandteil und Voraussetzung zur endgültigen Zulassung der Komponenten.

Trends



7 Trends

Die künftige Sicherheitslage hängt nicht nur von technischen, sondern verstärkt auch von gesellschaftlichen und wirtschaftlichen Entwicklungen ab. Auch rechtliche Trends, die sowohl aus den aktuellen Sicherheitsbedürfnissen hervorgehen als auch die Lage mit beeinflussen, spielen eine wichtige Rolle. IT-Sicherheit als isolierte Materie existiert nicht. Im Lagebericht 2007 wurden Trends vorgestellt, die nach Ansicht des BSI die Bedeutung von IT-Sicherheit auf verschiedene Weise hätten beeinflussen können. Von diesen sind bereits einige längst keine Trends mehr, sondern gehören fest zum Alltag – ein Beispiel ist das Thema Web 2.0. Andere Tendenzen haben sich wiederum als weitgehend bedeutungslos erwiesen und sind 2009 durch neue Trends, die ihrerseits möglicherweise künftig relevant sein werden, abgelöst worden.

7.1 Wirtschaftliche und gesellschaftliche Trends

Hypervernetzung

Die Tendenz geht dahin, dass Berufstätige immer und überall erreichbar sind. Bereits 16 Prozent der Arbeitnehmer weltweit sind „hypervernetzt“, das heißt, sie nutzen regelmäßig mindestens sieben digitale Geräte wie zum Beispiel Laptop, PDA und Handy sowie mindestens neun Anwendungen wie beispielsweise Instant Messaging, SMS, E-Mail und Web Conferencing. Technischer Fortschritt und demographische Veränderungen innerhalb der Arbeitnehmerschaft lassen einen Anstieg der Hypervernetzten auf über 40 Prozent in den kommenden fünf Jahren erwarten.[19] Und nicht nur im beruflichen, sondern auch im privaten Umfeld steigt die Nutzung mobiler Endgeräte und Anwendungen (vgl. Kapitel 5.2). Eine derartige Entwicklung führt aufgrund neuer Angriffspotenziale zu erhöhten Sicherheitsanforderungen – nicht nur auf Seiten der Hersteller und Anbieter mobiler Lösungen, sondern auch auf Seiten der Nutzer.

Green IT

Im Zusammenhang mit umweltpolitischen Themen und der aktuellen Klimaschutzdebatte rücken auch Umweltbestrebungen der IT-Industrie verstärkt in den Vordergrund. Dies ist zum einen auf das gesteigerte Umweltbewusstsein der Verbraucher zurückzuführen. Zum anderen sind vor allem – sowohl aus Anwender- als auch Herstellersicht – Kostenfaktoren für die Suche nach Energiesparpotenzialen verantwortlich.

Für die IT-Sicherheit schafft die so genannte Green IT neue Herausforderungen. Beispielsweise setzt ein Ansatz auf die Senkung des Energieverbrauchs mittels Leistungsreduzierung von IT-Systemen, was wiederum deren Verfügbarkeit beeinträchtigen könnte.

Auch die Entwicklung energiesparender Hard- und Softwarekomponenten birgt – wie alle neuen Techniken – neue Risiken. Maßnahmen, um den Energieverbrauch zu reduzieren, sollten daher stets mit dem Sicherheitsmanagement eines Unternehmens abgestimmt werden, da es auch sicherheitsrelevante Nebeneffekte geben kann.

Software as a Service (SaaS)

Weltweit steigt die Nachfrage nach Software as a Service (SaaS), oftmals auch als Softwaremiete oder Leasing bezeichnet, kräftig an. Prognosen gehen davon aus, dass bis zum Jahr 2012 mindestens ein Drittel aller Unternehmensanwendungen auf SaaS basieren, statt auf Produktlizenzen.[20] Dies bedeutet, dass Nutzer nur noch für Services zahlen, die sie auch tatsächlich nutzen. Damit können sie ihre Ausgaben senken und einen Großteil des Investitionsrisikos auf die Provider übertragen. Mit dem Risiko geben die Anwender aber auch die Kontrolle über die Infrastruktur und die Applikationen ab. Neue Risiken entstehen etwa bezüglich Datenschutz, Sicherheit, Verfügbarkeit sowie Backup und Recovery.

7.2 Technik-Trends

Informations- und Kommunikationstechnologien nähern sich auch in Zukunft einander immer weiter an und werden zunehmend allgegenwärtig. IT-Sicherheit wird aufgrund dessen eine noch stärkere Bedeutung erlangen als bisher.

Sicheres Internet der Dinge – Internet of Things

Die RFID-Technologie wird heute primär für die funktechnische Identifikation von Objekten eingesetzt. Einen nächsten Innovationsschritt stellen „intelligente“ RFID-Transponder dar. Beispielsweise könnte der von der Fluggesellschaft am Koffergriff angebrachte Papieranhänger künftig mit einem RFID-Transponder versehen sein. Dieser ermöglicht nicht nur die funktechnische Identifikation und Ortung eines Koffers, sondern steuert durch Kenntnis der Routeninformation auch eigenständig seinen Logistikweg. Es entsteht das so genannte Internet der Dinge (Internet of Things, IoT). Dieses stellt ein weltweites System vernetzter und über ein Standard-Kommunikationsprotokoll eindeutig adressierbarer Objekte dar, die untereinander Informationen wie Identität, Position und Umgebungsinformationen austauschen.

Zieht man die Parallele zum bekannten Internet, so ist offenkundig, dass bei der Entstehung des IoT die IT-Sicherheit von Anfang an mit berücksichtigt werden muss, um die bekannten Schwachstellen des Internets zu vermeiden. Die Notwendigkeit von Sicherheitsanalysen zur Bestimmung neuer Gefährdungen existiert hier kurzfristig vor allem für bereits angedachte Implementierungen von Infrastrukturkomponenten wie zum Beispiel eines Object Name Services (ONS). Dieser ist, vereinfacht gesagt, verantwortlich dafür, dass zu jedem Objekt der realen Welt ein virtuelles Gegenstück im Internet gefunden werden kann. Er entspricht demnach in seiner Funktion etwa dem Domain Name System (DNS) des bisherigen Internets (vgl. Kapitel 5.5). Eine Manipulation des ONS aufgrund nicht sorgfältig entwickelter Zugriffskontrollmechanismen hätte dementsprechend direkt Auswirkungen auf die Interaktion physischer Objekte, was als neue Klasse von Bedrohungen angesehen werden kann.

Sicherheit in drahtlosen Sensornetzen

In vielen technischen Anwendungen, wie bei der Steuerung und Überwachung von Industrieanlagen, müssen Umgebungsdaten in einem größeren Gebiet erfasst und verarbeitet werden. Klassischerweise geschieht dies mithilfe von fest verbauten und verkabelten Sensoren, die Messdaten an einen Zentralrechner übermitteln, von dem diese dann ausgewertet werden können. Derartige Systeme müssen mit einem relativ hohen Aufwand installiert und gewartet werden. Drahtlose Sensornetze stellen hier eine technologische Alternative dar. Ein drahtloses Sensornetz besteht aus einer Anzahl von mit Sensorik ausgestatteten Kleinstrechnern (Sensorknoten), die über einen Funkkanal miteinander kommunizieren können. Diese Sensorknoten verfügen dabei typischerweise über einen einfachen Prozessor, wenig Speicher und einen begrenzten Energievorrat in Form einer Batterie oder eines Akkus. Große Vorteile von drahtlosen Sensornetzen sind die relativ geringen Kosten und der flexible Einsatz. Das Thema drahtlose Sensornetze erfährt derzeit ein stark zunehmendes Interesse: Sie erscheinen für eine Vielzahl von Einsatzgebieten wie beispielsweise in der Logistik, in der Verkehrsüberwachung, beim Katastrophenschutz oder bei der statischen Überwachung von Gebäuden und Brücken geeignet und werden derzeit erprobt. Drahtlose Sensornetze können somit einen entscheidenden Beitrag zur zivilen Sicherheit leisten.

Die Gewährleistung von IT-Sicherheit in Sensornetzen ist mit besonderen Herausforderungen verbunden. Sicherheitsmechanismen müssen unter Berücksichtigung der beschränkten Hardware- und Energieressourcen entworfen werden. Ebenso muss die Ad-Hoc-Vernetzung und die verteilte Verarbeitung der Daten beachtet werden. Außerdem besteht durch die funktechnische Kommunikation ein großes Manipulationspotenzial. Eine frühe Auseinandersetzung mit diesem Thema ist angesichts der absehbaren weiteren Verbreitung besonders wichtig. Die Entwicklung von Leitlinien zur sicheren Konfiguration und zum sicheren Betrieb von Sensornetzen ist gerade auch zur Steigerung der zivilen Sicherheit unverzichtbar.

Biometrie in Kombination mit Kryptographie

Ein wichtiges zukünftiges Einsatzgebiet der Biometrie ist der Ersatz von Passwörtern als Zugangsberechtigung zu Rechnersystemen. Das in klassischen Passwort-Authentikations-Systemen erfolgreich praktizierte Verfahren, nur einen Hash-Wert des Passwortes als Referenzwert zu speichern, der keine Rückschlüsse auf das eigentliche Passwort erlaubt, scheidet bei biometrischen Verfahren aufgrund der verwendeten Abbildungsfunktionen für biometrische Merkmale aus. Die aktuelle Forschung befasst sich daher mit der Fragestellung, wie die Vorteile der Biometrie mit bewährten Verfahren der Kryptographie effektiv zu

kombinieren sind, so dass das ursprüngliche biometrische Merkmal in Analogie zum Passwort-Verfahren nicht mehr im Klartext, sondern als öffentlicher Referenzdatensatz gespeichert werden kann. Eine wesentliche Zielsetzung dieser Ansätze ist die Nutzung biometrischer Daten als kryptographische Schlüssel, ohne die Daten selbst im Klartext zu verwenden. Damit eine Kompromittierung oder Rekonstruktion des originären biometrischen Merkmals bzw. des gewonnenen Schlüssels nicht möglich ist, müssen starke Schlüssel verwendet werden, die nicht gebrochen werden können. Die Forschung sucht also nach geeigneten Kombinationen von Multibiometrie und Kryptographie, um genügend individuelle Daten zur Generierung starker Schlüssel für kryptographisch-biometrische Authentifizierungssysteme zu gewinnen.

Quantencomputerresistente Kryptoverfahren und Quantenkryptographie

In den vergangenen Jahren hat es erhebliche Fortschritte in der Grundlagenarbeit zur Realisierbarkeit von Quantencomputern gegeben. Falls Quantencomputer in einer bestimmten Größenordnung technisch realisiert werden, können sie ganz bestimmte Aufgaben wesentlich effizienter erledigen als herkömmliche Computer. Viele der zurzeit gängigen kryptographischen Algorithmen, die gegenwärtig Vertraulichkeit, Integrität und Authentizität sicherstellen, wären dann faktisch gebrochen. Vor allem im Hinblick auf Daten, deren Vertraulichkeit langfristig gewährleistet werden soll, ist es notwendig, dass sich die Forschung bereits heute mit dieser Thematik befasst. Es werden kryptographische Algorithmen benötigt, die den potenziellen Zusatzrisiken durch Quantencomputer widerstehen, gleichzeitig gegen klassische Angriffe resistent sind und zudem effizient technisch realisiert werden können. Im Bereich der Quantenkryptographie, welche die Eigenschaften der Quantenmechanik positiv als Basis für Sicherheitslösungen nutzt, sind Forschung und Entwicklung schon deutlich weiter.

Kryptographische Hashfunktionen

Kryptographische Hashwerte spielen unter anderem bei der Erstellung digitaler Signaturen eine zentrale Rolle. Bereits im Lagebericht 2007 wurde von Schwachstellen im weltweit verbreiteten und von der US-Behörde National Institute of Standards and Technology (NIST) standardisierten SHA-1 Algorithmus berichtet. Mittlerweile ist der Einsatz von SHA-1 zur Erzeugung qualifizierter elektronischer Signaturen gemäß Signaturgesetz nicht mehr erlaubt. NIST hat einen Wettbewerb ausgerufen, um einen neuen Hash-Standard festzulegen. Die Frist zur Einreichung von Vorschlägen zu Algorithmen endete im Oktober 2008. Nach derzeitigen Planungen könnte der neue Standard Ende 2012 in Kraft treten. Bis dahin werden primär Vertreter der SHA-2-Familie zum Einsatz kommen, die auch zur Erzeugung von gesetzeskonformen qualifizierten Signaturen erlaubt sind.

7.3 Rechtliche Trends

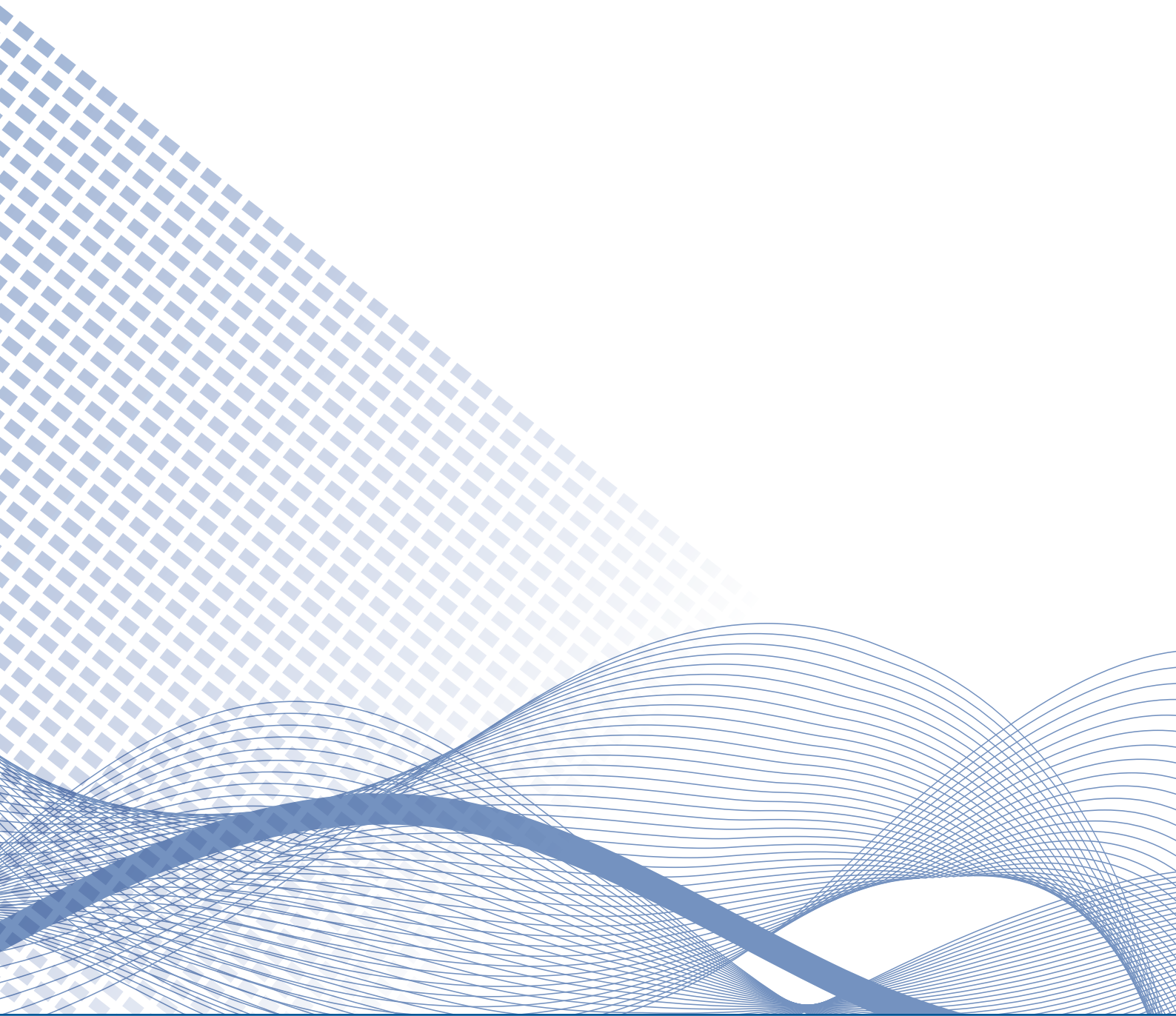
Aufgrund gestiegener Kriminalität im IT-Bereich ist auch eine zunehmende Zahl von Rechtsstreitigkeiten mit IT-Hintergrund zu verzeichnen. Nach der gegenwärtigen Rechtslage bereitet zum einen die lediglich vereinzelt bestehende spezialgesetzliche Normierung von Sicherheitspflichten Schwierigkeiten. Zum anderen ist die Zersplitterung der Thematik in eine Vielzahl von Einzelgesetzen problematisch. Einheitliche Regelungen oder ein übergreifender Ansatz zur Gewährleistung einer grundlegenden IT-Sicherheit existieren bislang nicht. Daher wird vorwiegend auf die Auslegung allgemeiner Regelungen des bürgerlichen sowie des öffentlichen Rechts zurückgegriffen, die jedoch meist nicht die teilweise komplexen technischen Rahmenbedingungen berücksichtigen.

Finanzielle Schäden muss derzeit in der Regel der Geschädigte tragen. Bei ihm liegt auch die Beweislast für die Fehlerhaftigkeit der Software bzw. der Nachweis eines Zusammenhangs zwischen fehlerhaftem Produkt und Rechtsgutverletzung. IT-Hersteller und -Dienstleister haften nur begrenzt für Programm-Schwachstellen oder Sicherheitsmängel, da ein Datenverlust oder ein Produktionsausfall außerhalb von Vertragsbeziehungen regelmäßig nicht zu Ersatzansprüchen führt. Zudem gibt es zugunsten der Provider zahlreiche Haftungsbegrenzungen, so dass für IT-Hersteller und -Dienstleister lediglich eingeschränkte Anreize zur Einhaltung von Sicherheitsmaßnahmen bestehen. Technisch mögliche Schutzmaßnahmen werden vielfach nicht oder nur eingeschränkt getroffen, da diese mit zusätzlichen Kosten oder funktionalen Einschränkungen verbunden sind. Ziel der nächsten Jahre sollte sein, durch eine gesetzliche Regelung Anreize für IT-Hersteller und -Dienstleister zu schaffen, um geeignete Maßnahmen zur Verminderung von IT-Risiken zu entwickeln und ein erhöhtes IT-Sicherheitsniveau zu erzielen.

Aufgrund der steigenden Bedeutung von IT-Sicherheit wird es künftig verstärkt gesetzliche Vorgaben und Standards geben, die vorschreiben, dass und wie IT-Sicherheit bei Produkten und Dienstleistungen zu implementieren ist. Dazu gehören Gesetze aus dem hoheitlichen Bereich wie zum Beispiel das Passgesetz, aber auch Bereiche aus der Wirtschaft wie beispielsweise die Fahrpersonalverordnung (bzgl. des digitalen Fahrtenschreibers).



Aktivitäten



8 Aktivitäten

Auch wenn das Bewusstsein für die Notwendigkeit von IT-Sicherheit über alle gesellschaftlichen Gruppen hinweg gestiegen ist, kann dennoch von keiner Entspannung der Lage die Rede sein. Die immer perfideren Tricks der Internetkriminellen einerseits und die Zunahme von Online-Aktivitäten andererseits bedingen weiterhin eine intensive Auseinandersetzung mit dem Thema. Es gilt, IT-Sicherheit in der öffentlichen Diskussion eine kontinuierliche Präsenz zu sichern, um so einen Beitrag zur Lösung des Problems zu leisten.

8.1 Bürger

Das Thema IT-Sicherheit hat für viele Bürger an Bedeutung gewonnen, jedoch werden die zu treffenden Maßnahmen oftmals noch als zu zeit- und kostenintensiv erachtet. Das BSI versucht Bürgerinnen und Bürgern die Auseinandersetzung mit der Problematik zu erleichtern. Es stellt Hilfsmittel bereit, die speziell auf die heterogene Gruppe der Privatanwender und ihre Bedürfnisse zugeschnitten sind.

Im Jahr 2008 konnte das BSI das fünfjährige Jubiläum seines Online-Informationsangebots www.bsi-fuer-buerger.de feiern. Pünktlich dazu wurden die dazugehörigen Webseiten überarbeitet. Zusätzlich zu umfangreichen Informationen rund um das Thema IT-Sicherheit sind nun vermehrt auch Checklisten und anschauliche Kurzfilme verfügbar. Mit dem vierzehntäglich erscheinenden Newsletter „Sicher ◦ Informiert“ sowie der Extraausgabe bei zeitkritischen Sicherheitsvorfällen kommt das BSI dem Wunsch der Bürger nach kompetenten, gezielten und vor allem zeitnahen Informationen zu bestehenden Sicherheitsrisiken entgegen. Beide Services können über die Plattform www.buerger-cert.de abonniert werden. Des Weiteren bietet das BSI zahlreiches Informationsmaterial wie Broschüren und Flyer für Privatanwender an. Dieses wird sowohl in Schulen und in der Erwachsenenbildung als auch verstärkt im Unternehmensumfeld zur Sensibilisierung der Mitarbeiter genutzt. Auf Messen und Veranstaltungen haben Bürgerinnen und Bürger zudem die Möglichkeit, sich bei BSI-Mitarbeitern zu allen Aspekten rund um das Thema IT-Sicherheit zu informieren.

Gemeinschaftliches Handeln

Eine IT-Sicherheitskultur zu etablieren ist ein Ziel, das nicht von einer Behörde im Alleingang realisiert werden kann. Das BSI setzt bei seiner Ansprache

von Bürgerinnen und Bürgern daher auch verstärkt auf den Austausch und die Zusammenarbeit mit Kooperationspartnern und Multiplikatoren, die sich ebenfalls intensiv mit dem Thema IT-Sicherheit befassen. Auf diese Weise ist es möglich, die unterschiedlichen technischen, pädagogischen und psychologischen Aspekte der IT-Sicherheit kompetent und umfassend zu adressieren. Des Weiteren ist das BSI Beiratsmitglied des 2006 als Public Private Partnership gegründeten Vereins Deutschland sicher im Netz e.V. (DsiN). Mit konkreten Aktionen und Services bietet DsiN Kindern und Jugendlichen, Verbrauchern sowie kleinen und mittelständischen Unternehmen Hilfestellung und praktische Lösungen rund um IT-Sicherheit an. Das BSI unterstützt aktiv die Arbeit des Vereins. Auch auf internationaler Ebene ist das BSI im Bereich Aufklärung und Sensibilisierung für IT-Sicherheitsthemen tätig. So beteiligt sich das BSI in der Awareness Raising Community der ENISA (European Network and Information Security Agency) und ist mit Aktionen beim Aktionstag „Safer Internet Day“ vertreten, der von der Europäischen Union jährlich initiiert wird.

Vom technischen Standpunkt aus bietet die Einführung des elektronischen Personalausweises zudem einen zusätzlichen Sicherheitsgewinn. Die eID-Funktion zum Nachweis der digitalen Identität des Ausweisinhabers ermöglicht es, Daten, die auf dem elektronischen Personalausweis gespeichert sind, zur Online-Authentisierung zu verwenden. Er liefert damit verlässliche digitale Identitätsnachweise. Bürger können sich so besser vor Identitätsdiebstahl oder unfreiwilliger Datenerhebung schützen. Im Geschäftsverkehr mit Verwaltung und Wirtschaft, wie beispielsweise beim Online-Banking oder E-Commerce, lassen sich Ausweisinhaber mit dem elektronischen Personalausweis einfach und sicher identifizieren. Auch im Projekt Bürgerportale, dem Konzept zur sicheren und vertraulichen Kommunikation im Internet, wird die eID-Funktion zum Einsatz kommen und dafür sorgen, dass E-Mails zuverlässig und geschützt versendet werden können.

8.2 Wirtschaft

Der Nutzen von IT-Sicherheitsmaßnahmen ist schwer zu messen: Der Verlust von Daten oder der Ausfall eines Rechenzentrums infolge eines Angriffs auf ein Unternehmen verursachen hohe Kosten. Wenn es um die Sicherheit von Know-how und Daten geht, erkennen Unternehmer ihren Schutzbedarf oft erst nach einem Angriff. Um das Sicherheitsniveau in Unternehmen zu fördern und weiterzuentwickeln, stellt das BSI Informationsmaterialien für Firmen bereit. Zu nennen sind beispielsweise Broschüren und Leitfäden zu unterschiedlichen Aspekten der IT-Sicherheit, die von der Webseite www.bsi.bund.de heruntergeladen werden

können. Mit den IT-Grundschutz-Standards bietet das BSI zudem Informationen zu Themenbereichen an, die von grundsätzlicher Bedeutung für die Informationssicherheit in Unternehmen oder Behörden sind. Diese können die Empfehlungen des BSI nutzen und an ihre eigenen Anforderungen anpassen.

Das BSI ist auf zahlreichen Veranstaltungen und Messen im In- und Ausland vertreten und präsentiert dort Unternehmen und Behörden sein breites Angebot. Außerdem findet in Berlin regelmäßig eine Gesprächsreihe statt, die sich an Entscheider in Wirtschaft, Verwaltung und Wissenschaft richtet. Ziel ist es, mit hochrangigen Repräsentanten eines Sachgebiets einen meinungsbildenden Dialog anzustoßen, der absehbare Zukunftsthemen umreißt.

Ein weiterer Schwerpunkt des BSI ist die Zertifizierung von IT-Produkten und -Systemen. Die Nachfrage ist im vergangenen Jahr deutlich gestiegen. Zertifizierungen gemäß der international anerkannten Common Criteria schaffen Transparenz und Vergleichbarkeit sowohl für die Hersteller als auch für die Kunden und können für die Marktpositionierung eines Produkts von Vorteil sein. Der Einsatz zertifizierter Informationstechnik erhöht zudem das IT-Sicherheitsniveau und kann zum Schutz gegen Angriffe auf die Unternehmensinfrastruktur beitragen. Das BSI zertifiziert ebenfalls nach ISO 27001 auf Basis von IT-Grundschutz. Ein Unternehmen kann so zum Beispiel gegenüber Kunden belegen, dass der Umgang mit IT-Risiken bestimmten Anforderungen entspricht. Das BSI trägt mit seinen Aktivitäten im Bereich der Zertifizierung zur Erhöhung des IT-Sicherheitsniveaus in Deutschland bei.

Kritische Infrastrukturen (KRITIS)

Der im September 2007 verabschiedete Umsetzungsplan KRITIS (UP KRITIS) legt in seiner „Roadmap“ wesentliche Schritte zur weiteren Verbesserung der IT-Sicherheit in den Kritischen Infrastrukturen Deutschlands fest: Die am UP KRITIS beteiligten Vertreter der privatwirtschaftlich betriebenen Kritischen Infrastrukturen und zuständige Behörden wie das BSI bereiten sich in Arbeitsgruppen gemeinschaftlich auf den Umgang mit IT-bedingten Vorfällen und IT-Krisen vor.

Die Arbeitsgruppen entwerfen sektorübergreifende IT-Krisenszenarien und dazu passende Übungen. Erste Planuntersuchungen und Kommunikationsübungen wurden bereits durchgeführt. Des Weiteren werden Vorgehensweisen für die Reaktion auf sektorübergreifende IT-Krisen entwickelt. Hierzu wird zum Beispiel ein Netz von Single Points of Contact (SPOCs) für anlassbezogene Kommunikation sowie zur Alarmierung und Krisenbewältigung aufgebaut. Erste SPOCs sind bei der Versicherungs-, der Kredit- sowie der Mineralölwirtschaft im Aufbau. Mit den 2008 fertig gestellten Rahmenkonzepten zu Krisenreaktion und Übungen wurden die Eckpunkte der weiteren Zusammenarbeit festgelegt.

Ab 2009 werden die Aktivitäten zur „Aufrechterhaltung kritischer Infrastrukturdienstleistungen“ verstärkt. Besonders wichtige Prozesse und Komponenten innerhalb der Kritischen Infrastrukturen werden ermittelt, um die Stabilität der Dienstleistungen durch Schutzmaßnahmen und angepasste Krisenreaktionsmechanismen weiter verbessern zu können.


Auf internationaler Ebene liegt das Hauptaugenmerk auf dem Informationsaustausch zum Europäischen Programm zum Schutz Kritischer Infrastrukturen (EPSKI) sowie auf Untersuchungen zur Bestimmung geeigneter Kriterien, um europäische Kritische Infrastrukturen im IKT-Sektor zu identifizieren.

8.3 Verwaltung

Mit dem Umsetzungsplan Bund (UP Bund) wurde gegen Ende 2007 erstmals eine einheitliche IT-Sicherheitsleitlinie für sämtliche Ressorts verabschiedet. Im UP Bund sind technische, organisatorische und prozessuale Standards für die Bundesverwaltung festgeschrieben, die in allen Behörden der Bundesverwaltung durch angemessene IT-Sicherheitsmaßnahmen realisiert werden.

Das BSI unterstützt hier die Bildung und Aufrechterhaltung der zugrunde liegenden Sicherheitsprozesse. Dies geschieht im strategischen und konzeptionellen Bereich durch Bereitstellung zahlreicher Hilfsmittel. Von zentraler Bedeutung sind hier natürlich die überarbeiteten BSI-Standards sowie die ständig aktualisierten IT-Grundschutzkataloge. Zur kontinuierlichen Aufrechterhaltung der Sicherheitsprozesse werden auch Hilfsmittel zur Informationssicherheitsrevision bereitgestellt.

Konkrete Hilfestellung leistet das BSI durch Konzeption und Durchführung einer Schulungsreihe für IT-Sicherheitsbeauftragte in Behörden an der Bundesakademie für die öffentliche Verwaltung (BAköV). Die Definition des Jobprofils „IT-Sicherheitsbeauftragter“ und dessen Ausbildung mit Erwerb eines Zertifikats schafft Struktur in Verantwortung und Kompetenz. Ende 2008 waren 70 Absolventen zertifiziert. Die dreiwöchigen Schulungsmaßnahmen finden mehrmals im Jahr statt. Zu erwarten ist, dass durchschnittlich 50 zertifizierte Absolventen jedes Jahr hinzukommen. Des Weiteren bietet das BSI ein Beratungskonzept an, dass insbesondere die IT-Sicherheitsbeauftragten der Behörden in ihrer täglichen Arbeit unterstützt.



Im operativ technischen Bereich werden die schon etablierten Schutzmaßnahmen weiter ausgebaut. Um IT-Krisen wirkungsvoll begegnen zu können, werden Frühwarnsysteme und Krisenreaktionsprozesse ständig optimiert. Mit CERT-Bund hat das BSI eine zentrale Anlaufstelle für präventive und reaktive Maßnahmen in Bezug auf sicherheits- und verfügbarkeitsrelevante Vorfälle in Computersystemen, deren Dienstleistungen in erster Linie Bundesbehörden zur Verfügung stehen.

In Anbetracht der gestiegenen Bedrohungslage der vergangenen Jahre werden die bedeutendsten Netzinfrastrukturen der Bundesverwaltung, der Informationsverbund Berlin-Bonn (IVBB) und der Informationsverbund der Bundesverwaltung (IVBV), weiterentwickelt.

8.4 Zukunftsfonds

Eine intensive Forschung ist unerlässlich, um der sich ändernden Bedrohungslage präventiv entgegenzutreten. In seinem eigenen IT-Sicherheitsforschungsprogramm (Zukunftsfonds), das aus dem 6 Milliarden-Programm der Bundesregierung finanziert wird, behandelt das BSI prioritäre Fragestellungen auf dem Gebiet der IT-Sicherheit. Das Programm dient dem Ziel, anwendungsbezogene Innovationen – vor allem in den Technologiefeldern Internet-Frühwarnsysteme, Trusted Computing sowie Biometrie und Ausweissysteme – zu erarbeiten und in die Anwendung zu überführen. Um eine nachhaltige Wirkung der Ergebnisse zu erzielen, ist eine enge Kooperation und Verzahnung der Behörden als Bedarfsträger auf der einen Seite und mit den Auftragnehmern aus Forschung und Wirtschaft auf der anderen Seite nötig.

Fazit



9 Fazit

Der vorliegende Bericht zur Lage der IT-Sicherheit in Deutschland verdeutlicht die unverändert ernst zu nehmende Bedrohungslage. Einige Angriffsmethoden werden bei Internetkriminellen immer beliebter, während andere an Bedeutung verlieren. Fakt ist, dass Tag für Tag Tausende neue Schadprogramme das Internet überschwemmen.

Hinzu kommen neue Technologien, deren Risikopotenzial heute zwar schwer abschätzbar ist, jedoch mit zunehmender Verbreitung und Akzeptanz vermutlich steigen wird. Die folgenden Tabellen illustrieren eine zeitliche Dynamik verschiedener Gefährdungstrends. Auf Basis sorgfältiger Recherchen und Erhebungen werden künftige Entwicklungen prognostiziert.

Gefährdungstrends

Bedrohung	2007	2009	Prognose
Zero Day Exploits	↑	↑	→
Drive-by-Downloads	—	↑	↑
Trojanische Pferde	↑	↑	↑
Viren	↓	↓	→
Würmer	↓	↓	→
Spyware	↑	↑	→
DDoS-Angriffe	→	↑	↑
Unerwünschte E-Mails	↑	↑	↑
Bot-Netze	→	↑	↑
Identitätsdiebstahl	↑	↑	↑
Betrügerische Webangebote	—	↑	→
Abstrahlung	—	→	→
Materielle Sicherheit, Irrtum, Nachlässigkeit	→	↑	→

 Gefährdung nimmt zu
  gleichbleibende Gefährdung
  Gefährdung sinkt

Quelle: BSI

Abbildung 11: Entwicklung von IT-Bedrohungen nach Einschätzung des BSI [6]

Risikopotenzial für Angriffsmöglichkeiten in ausgewählten Anwendungen und Technologien

Technologie / Anwendung	2007	2009	Prognose
Voice over IP	↑	→	→
Mobile Datenübertragung	—	↑	↑
Web 2.0	—	↑	↑
SCADA	→	↑	↑
DNS	—	↑	↑
Multifunktionsgeräte	—	↑	→
Schnittstellen und Speichermedien	—	↑	→
Netzkoppelemente	—	↑	↑
SOA	—	↑	↑

 Gefährdung nimmt zu
  gleichbleibende Gefährdung
  Gefährdung sinkt

Quelle: BSI

Abbildung 12: Risikopotenzial für Angriffsmöglichkeiten in ausgewählten Anwendungen und Technologien nach BSI-Einschätzung [6]

Risikoprofil innovativer Anwendungen und Technologien

Technologie / Anwendung	2007	2009	Prognose
RFID	→	→	↑
Biometrie und Personaldokumente	—	↑	↑
IPv6	—	↑	→
Automotive	—	↑	↑
Gesundheitskarte	—	↑	→

 Gefährdung nimmt zu
  gleichbleibende Gefährdung
  Gefährdung sinkt

Quelle: BSI

Abbildung 13: Risikoprofil innovativer Anwendungen und Technologien nach Einschätzung des BSI [6]


Sicher ist, dass Internetkriminalität ein profitables Geschäft ist. Dort, wo Gewinne zu erwarten sind, wird es zahlreiche Nachahmer geben. Immer mehr Transaktionen, die über das Internet abgewickelt werden, führen zusätzlich dazu, dass das Gefährdungspotenzial steigt.

Aber es gibt auch positive Entwicklungen. Erfreulich ist, dass das Sicherheitsbewusstsein in Verwaltung, Wirtschaft und Gesellschaft zunimmt. Dass IT-Sicherheit zugleich einen Schutz des Unternehmenswertes bzw. des Privateigentums bedeutet, veranlasst eine Vielzahl von Anwendern und Institutionen dazu, Schutzmaßnahmen für ihre Systeme zu ergreifen. Offenbar sind Nutzer besser mit technischen Sicherheitsvorkehrungen vertraut als noch vor einigen Monaten. Doch den immer heimtückischer werdenden Angriffen von Kriminellen entgegenzuwirken, erfordert auch ein immer höheres Maß an IT-Sicherheitskompetenz. Nur wenn diese Kompetenz aufrechterhalten und kontinuierlich ausgebaut wird, kann ein wirkungsvoller Schutz der Anwender und ihrer Systeme in Gesellschaft, Wirtschaft und Verwaltung erreicht werden.

Technisches Verständnis und technische Absicherung allein sind jedoch nicht ausreichend. Die Beispiele hinsichtlich zunehmender psychologischer Manipulation zeigen, wie wichtig es ist, dass Internetnutzer auch ihr Verhalten und das Maß an persönlichen Daten, die sie beispielsweise in Social Networks zur Verfügung stellen, reflektieren. Bezüglich ihres eigenen Datenschutzes sind die Anwender jedoch oftmals nachlässig.

Aus dem gleichen Grund gilt auch für Unternehmen und Behörden: Der Schutz von Unternehmensinformationen endet heute nicht mehr an der Pforte. Die Werkstore sind virtuell geworden. Neben dem Einsatz technischer Schutzvorrichtungen ist eine umfangreiche Sensibilisierung der Mitarbeiterinnen und Mitarbeiter beim Gebrauch der IT-Geräte und im Umgang mit Unternehmensinformationen unerlässlich. Ein zusätzliches Problem im wirtschaftlichen Umfeld ist der Aspekt der Spionage, um Wettbewerbsvorteile gegenüber Konkurrenten realisieren zu können. Ganzheitliche Sicherheitskonzepte, welche die nötigen personellen und finanziellen Ressourcen in angemessener Weise berücksichtigen, sind unverzichtbar, um eine Institution dauerhaft vor Schäden zu bewahren.

Angesichts der in diesem Bericht dargelegten Angriffsmöglichkeiten ist zudem eine umfassende IT-Sicherheitsforschung erforderlich. Die IT-Sicherheitsindustrie handelt heute meist reaktiv: Erst beim Auftreten neuer Sicherheitslücken, neuer Viren oder neuer Trojanischer Pferde wird ein entsprechender Patch oder ein Update erarbeitet und ausgeliefert. In Zukunft sollte die nachhaltige, anwendungsorientierte IT-Sicherheitsforschung durch vorbeugende Maßnahmen verbessert werden. Diese Problematik ist nicht allein im unternehmerischen



oder unternehmensnahen Umfeld begründet. Eine rein akademische Forschung erscheint jedoch aufgrund oftmals theoretischer Konzepte ebenfalls nicht ausreichend geeignet, um die Informationstechnik in der Praxis sicherer zu gestalten. Die Situation stellt sich dennoch recht positiv dar. Es gibt in Deutschland im Bereich der IT-Sicherheitsforschung eine Vielzahl von Ansätzen, bei denen Wirtschaft, Universitäten und Einrichtungen der öffentlichen Verwaltung miteinander kooperieren.

Nicht zuletzt bleibt aber auch der Anwender selbst gefordert. Verantwortungsvoller und umsichtiger Umgang mit Informationstechnik und Daten ist ein wichtiger Faktor, um das Sicherheitsniveau dauerhaft zu erhöhen. Der mündige Bürger kann dies nicht allein an Staat und Provider delegieren. Gemeinsame Ziele erfordern gemeinschaftliches Handeln. Nur so lässt sich die Basis für eine langfristig sichere Nutzung von Informationstechnik schaffen und Internetkriminalität wirkungsvoll entgegenzutreten.



10 Quellen

- [1] (N)ONLINER Atlas 2008, TNS Infratest GmbH und Initiative D21 (Hrsg.).
- [2] internet facts 2008-I, Arbeitsgemeinschaft Online-Forschung e.V.
- [3] BITKOM Presseinformation vom 6. Juli 2008.
- [4] 4. ePerformance Report 2008 – Sonderbericht zum Dritten Nationalen IT-Gipfel, Bundesministerium für Wirtschaft und Technologie (Hrsg.).
- [5] IT-Trends 2008, Capgemini.
- [6] BSI-Erhebungen.
- [7] IT-Security 2008, InformationWeek.
- [8] IT-Security-Agenda 2007+ - Schlüsselthemen und Trends in Deutschland, Experton Group AG.
- [9] kes/Microsoft-Sicherheitsstudie 2008.
- [10] Secunia Monthly Report, October 2008.
- [11] Sophos Security Threat Report, Q1 2008.
- [12] Bundeskriminalamt.
- [13] Studie: Industriespionage, Corporate Trust GmbH, 2007.
- [14] Bundesnetzagentur, <http://www.bundesnetzagentur.de/media/archive/14234.pdf>.
- [15] ARD/ZDF-Online-Studie 2008.
- [16] WhiteHat Website Security Statistics Report, März 2008.
- [17] Secure USB Flash Drives, ENISA, 2008.



[18] Securitytracker, <http://www.securitytracker.com/topics/topics.html>.

[19] The Hyperconnected – Here They Come!, IDC/Nortel, 2008.

[20] Gartner, Inc. Presseinformation vom 31. Januar 2008.

11 Glossar

Bot / Bot-Netz

Bei einem Bot (Abk. für Roboter) handelt es sich um ein Programm, das auf dem Rechner eines Anwenders ohne sein Wissen installiert wird und aus der Ferne Anweisungen des Besitzers ausführt. Werden viele Bots zusammengeschlossen, so handelt es sich um ein Bot-Netz.

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.

Command-and-Control-Server (C&C-Server)

Command-and-Control-Server sind das zentrale Steuerelement eines Bot-Netztes.

DoS-Angriff

Denial of Service bedeutet so viel wie „außer Betrieb setzen“. Bei einem DoS-Angriff wird ein Computer von vielen anderen Rechnern mit Netzwerkpaketen oder Anfragen bombardiert. Der Rechner kann die gewaltigen Paketmengen oft nicht verarbeiten und wird überlastet. Starten mehrere Quellen gleichzeitig einen Angriff, spricht man von einem DDoS-Angriff (Distributed Denial of Service-Angriff).

Drive-by-Download

Drive-By-Download bezeichnet das automatische Herunterladen und Ausführen eines Schadprogramms beim Besuch einer Webseite. Der Schadcode wird dabei auf den Rechner geladen, ohne dass der Anwender dazu eine Aktion – wie das Anklicken eines Links oder einer Datei – ausführen muss. Das bloße Ansehen einer Webseite reicht somit aus, um den Rechner zu infizieren.

DVI-Schnittstelle

Digitale Schnittstelle zwischen Grafikkarte und Display. Die DVI-Schnittstelle löst die analoge Übertragung der VGA-Schnittstelle ab.

Estland- und Georgien-Vorfall

In mehreren Wellen wurden im Frühjahr 2007 schwere DDoS-Angriffe auf estnische Webseiten von Unternehmen, Banken, Behörden, Polizei und Regierung gestartet, die dadurch tagelang lahm gelegt waren. Im Herbst 2008 waren auch georgische Webseiten Ziel von DDoS-Angriffen. Webseiten staatlicher georgischer Stellen waren nicht mehr erreichbar.

Exploit

Programm zur Ausnutzung einer Schwachstelle in einer Software.

Firewire

Serielle Schnittstellentechnologie zur Übertragung digitaler Daten mit bis zu 400 Mbit/Sek. Firewire ist neben i.Link eine Bezeichnung für den IEEE (Institute of Electrical & Electronic Engineers)-Standard 1394.

Hashwert

Eine kryptographische Hashfunktion errechnet zum Beispiel aus einer Datei beliebiger Länge einen Bitstring fester Länge. Ein Hashwert wird auch als fingerprint (Fingerabdruck) bezeichnet. Die Zielsetzung: Es soll praktisch nicht möglich sein, zwei unterschiedliche Dateien angeben zu können, die den gleichen Hashwert besitzen.

Internet Relay Chat (IRC)

IRC bezeichnet einen virtuellen Treffpunkt zur textbasierten Echtzeit-Kommunikation.

iTAN

iTAN ist die Abkürzung für Indiziertes TAN-Verfahren. Bei iTAN muss eine bestimmte TAN aus einer Liste eingegeben werden. Die TAN ist an einen bestimmten Auftrag gebunden und kann nicht beliebig verwendet werden.

mTAN (auch smsTAN)

mTAN ist die Abkürzung für mobile TAN und wird auch als smsTAN bezeichnet. 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.

KRITIS – Kritische Infrastrukturen

Organisationen und Einrichtungen mit wichtiger Bedeutung für das staatliche Gemeinwesen, bei deren Ausfall oder Beeinträchtigung nachhaltig wirkende Versorgungsengpässe, erhebliche Störungen der öffentlichen Sicherheit oder andere dramatische Folgen eintreten würden.

Man-In-The-Middle-Attacke

Ein Angriff auf den Kommunikationskanal zwischen zwei oder mehreren kommunizierenden Personen bzw. Computersystemen. Der Angreifer versucht dabei, die Kommunikation unbemerkt unter seine Kontrolle zu bringen mit dem Ziel, die ausgetauschten Informationen nach seinem Belieben einsehen oder manipulieren zu können.

Peer-to-Peer-Netz (P2P-Netz)

Ein P2P-Netz ist eine Netzwerkstruktur, in der alle Kommunikationsteilnehmer gleichberechtigt sind und infolgedessen sowohl als Client als auch als Server fungieren können.

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 Übertragungstrecke 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.

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.

Single Point of Failure (SPoF)

Single Point of Failure bezeichnet eine einzelne Fehlerstelle. Es handelt sich um eine Komponente, deren Ausfall zu einem Ausfall des ganzen Systems führt.

Social Engineering

Im Zusammenhang mit IT-Sicherheit wird der Begriff für eine Strategie von Online-Betrügern gebraucht. Indem die Kriminellen 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, um beispielsweise Phishing-E-Mails persönlich zu formulieren und dadurch Vertrauen zu wecken.

SQL-Injection

Ausnutzen einer Sicherheitslücke in Zusammenhang mit SQL-Datenbanken. Sind Webanwendung und Datenbank nicht sorgfältig programmiert, kann ein Angreifer über diese Eingabefelder – statt der erwarteten Daten – Befehle an die Datenbank eingeben („Injection“). Auf diese Weise lassen sich beispielsweise Informationen oder Links in Webseiten verändern.

VGA-Schnittstelle

Schnittstelle zwischen Grafikkarte und Display, bei dem drei analoge Videosignale für Rot, Grün und Blau sowie Synchronisationssignale übertragen werden.

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.

Zero-Day-Exploit

Die Ausnutzung (Exploit) einer Sicherheitslücke vor oder am gleichen Tag der öffentlichen Bekanntmachung.

Herausgeber

Bundesamt für Sicherheit in der Informationstechnik - BSI
53175 Bonn

Texte und Redaktion

Bundesamt für Sicherheit in der Informationstechnik
pressto GmbH – Agentur für Medienkommunikation, Köln

Layout und Gestaltung

artwork factory kommunikation & design, Köln

Druck

Das Druckhaus Bernd Brümmer, Alfter

Stand

Januar 2009

Bezugsstelle

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