4.3.1 IT-Sicherheit

Entwicklungen im Bereich IT-Sicherheit

Die Konvergenz der Informations- und Kommunikationstechnologien (IKT) wird über 2015 hinaus weiter an Bedeutung gewinnen und in nahezu allen Sektoren der Wirtschaft eine dominierende Rolle spielen. Auch im Bereich der IKT-Sicherheit zeichnen sich besondere Entwicklungen ab, wie die Studie „Technologische und wirtschaftliche Perspektiven Deutschlands durch die Konvergenz der elektronischen Medien“ zeigt. Demnach wird sich die IT-Sicherheit neuen Herausforderungen stellen müssen:

- Durch neue Anwendungen wie beispielsweise Cloud Computing oder auch durch die zunehmende Verbreitung des Web 3.0 (semantisches Web) nehmen die Sicherheitsrisiken rasch zu und bieten sich vermehrt Angriffspunkte für Kriminelle. Die IT-Sicherheitsbranche muß darauf schnell reagieren.

- Die Berechenbarkeit von komplexen Angriffen auf kritische Infrastrukturen wird aber durch neue IT-gestützte Identifizierungsmöglichkeiten von Schwachstellen oder durch mögliche neue mobile Administrationslösungen einfacher handhabbar.

- Sicherheitsrisiken und -lücken können künftig umfänglich nur in enger Zusammenarbeit zwischen der öffentlichen Verwaltung und den Wirtschaftsunternehmen durch Public Private Partnerships beherrscht werden.

- Das Management und die Vernetzung der IT-Sicherheit werden eine zentrale Aufgabe der öffentlichen Verwaltung, der Behörden und Organisationen mit Sicherheitsaufgaben und der Wirtschaft sein.

- Spezialexpertisen zur Gewährleistung von IT-Sicherheit (beispielsweise in Embedded Systems) müssen erst aufgebaut und Qualifizierungsengpässe beseitigt werden.

Maßnahmen der Politik: Die Cyber-Sicherheitsstrategie, De-Mail und der neue Personalausweis

Prävention und Schutz vor IT-Sicherheitsrisiken werden von der deutschen Politik als wichitge Aufgabe angesehen. Vor allem die sichere und nachweisbare De-Mail oder der neue Personalausweis sind zukunftsweisende Methoden, um sich vor Angriffen von Betrügern zu schützen. Der wichtigste Faktor beim Schutz der IT-Sicherheit ist aber nach wie vor die Aufklärung über Risiken und Sicherheit. In Deutschland leisten beispielsweise das Protal www.bsi-fuer-buerger.de des Bundesamts für Sicherheit in der Informationstechnik und die unter der Schirmherrschaft des Bundesministeriums des Innern stehende Initiative Deutschland sicher im Netz e. V. diese „aufklärerische Arbeit“.

Im Februar 2011 hat die Bundesregierung die Cyber-Sicherheitsstrategie beschlossen. Sie verfolgt zehn strategische Ziele und Maßnahmen:

1. Schutz kritischer Informationsinfrastrukturen
2. Sichere IT-Systeme in Deutschland
3. Stärkung der IT-Sicherheit in der öffentlichen Verwaltung
4. Nationales Cyber-Abwehrzentrum
5. Nationaler Cyber-Sicherheitsrat
6. Wirksame Kriminalitätsbekämpfung auch im Cyber-Raum
7. Effektives Zusammenwirken für Cyber-Sicherheit in Europa und weltweit
8. Einsatz verlässlicher und vertrauenswürdiger Informationstechnologie
9. Personalentwicklung der Bundesbehörden
10. Instrumentarium zur Abwehr von Cyber-Angriffen.

Das Nationale Cyber-Abwehrzentrum nahm am 1. April 2011 unter der Federführung des Bundesamtes für Sicherheit in der Informationstechnik (BSI) und mit direkter Beteiligung des Bundesamtes für Verfassungsschutz (BfV) sowie des Bundesamtes für Bevölkerungsschutz und Katastrophenhilfe (BBK) seine Arbeit auf. Das Cyber-Abwehrzentrum hat die Aufgabe, IT-Sicherheitsvorfälle schnell und umfassend zu bewerten und abgestimmte Handlungsempfehlun-

„2011 ist das Jahr der Einbrüche in IT-Netze. Die Medien berichten beinahe täglich von erfolgreichem Datenklau bei Weltkonzernen: Sony, Neckermann, Sega – selbst Unternehmen, deren originäres Produkt die ‚Sicherheit‘ ist, sind trotz Sicherheitsmaßnahmen vor Hackerangriffen nicht gefeit: HBGary, RSA, Comodo, Barracuda Networks, Bundespolizei, Zollkriminalamt. Die Löcher gilt es zu finden – ohne Penetrationstests hat man hier keine Chance.“

Sebastian Schreiber,
Geschäftsführer,
SySS GmbH

gen zu erarbeiten. Dazu werden unter anderem Informationen über Täterbilder sowie über Schwachstellen in IT-Produkten ausgetauscht sowie IT-Vorfälle, Verwundbarkeiten und Angriffsformen analysiert.

Vertrauen und IT-Sicherheit: Die Digitale Agenda in Europa

Vertrauen in die Sicherheit des Internets ist die zentrale Voraussetzung für seine intensivere Nutzung. Die von der Europäischen Kommission im Mai 2010 herausgegebene „Digitale Agenda für Europa“ sieht vielfältige Maßnahmen zur Stärkung der Sicherheit in der digitalen Gesellschaft vor. An Maßnahmen im IT-Sicherheitsbereich werden unter anderem vorgeschlagen:

- bis 2012: die Einrichtung einer europäischen Plattform zur Bekämpfung der Cyberkriminalität. Darunter fallen eine Verordnung zur Modernisierung der Europäischen Agentur für Netz- und Informationssicherheit (ENISA) sowie Vorschläge zur Einrichtung eines Computer-Notfallteams (CERT) für die EU-Organe;

- bis 2012: Vorschläge zur Einrichtung einer Online-Schlichtung bei Streitfällen um Zahlungen im elektronischen Geschäftsverkehr;

- bis 2012: Vorschläge zum Ausbau des Schutzes personenbezogener Daten;

- bis 2013: der Aufbau von Hotlines für die Meldung anstößiger und schädlicher Online-Inhalte an nationale Meldesysteme;

- bis 2015: Empfehlungen zur Einrichtung einer Online-Gerichtsbarkeit mit europäischer und weltweiter Zuständigkeit.

IT-Sicherheit in Unternehmen

Unternehmen haben ihre Daten und Netzwerke verstärkt vor Datendiebstahl, Insiderattacken und Angriffen aus dem Social Web zu schützen. Das haben 2011 die Hackerangriffe auf renommierte Unternehmen wie Neckermann und Sony oder öffentliche Einrichtungen wie den Deutschen Zoll oder den Internationalen Währungsfonds (IWF) erneut gezeigt.

Auch erfordern Bereiche wie Cloud Computing und Virtualisierung ganzheitliche IT-Sicherheitskonzepte. Drei Viertel der von IDC befragten Unternehmen verfügen darüber. Allerdings bemängeln 19 Prozent der Befragten konzeptionelle Lücken. 30 Prozent führen an, dass die Konzepte nur teilweise von den Mitarbeitern akzeptiert bzw. umgesetzt werden.

Häufig ist der direkte Schaden, der durch die Ausnutzung von Sicherheitslücken in Unternehmen entsteht, nicht der entscheidende. 48 Prozent der in der IDC-Studie „IT Security in Deutschland 2010“ befragten IT-Sicherheitsverantwortlichen geben an, dass Angriffe auf die IT-Sicherheit ihres Unternehmens zu Produktivitätsverlusten geführt hätten. Die betroffenen Unternehmen haben aber auch zu 39 Prozent mit personellen und zu 23 Prozent mit rechtlichen Konsequenzen zu kämpfen. Bei 22 Prozent haben die Angriffe auf die internen IT-Systeme Imageschäden zur Folge.

Das wichtigste Hemmnis, das einer ausreichenden IT-Sicherheit in den Unternehmen entgegenstand, ist das fehlende „Sicherheitsbewusstsein“ der Mitarbeiter.

Internet-Kriminalität nimmt weiter zu

Die Sicherheitsverletzungen im IKT-Bereich nehmen zu. Es werden vermehrt wirtschaftlich motivierte Angriffe beobachtet. Computer- oder Cyberkriminalität findet in organisierter Form statt. Wie die polizeiliche Kriminalstatistik für das Jahr 2010 zeigt, ist die Zahl der Cybercrime-Fälle in Deutschland, also Straftaten, die mit moderner Informations- und Kommunikationstechnik bzw. gegen sie begangen werden, um 19 Prozent auf fast 60.000 gestiegen. In fast 27.000 Fällen handelte es sich dabei um Computerbetrug (z.B. Phishing). Der registrierte Schaden, der durch die Internet-Kriminalität entstand, lag bei rund 61,5 Millionen Euro verglichen mit noch rund 37 Millionen Euro im Jahr 2009.

Verbraucher: Vermehrt schlechte Erfahrungen

Laut einer BITKOM-Umfrage aus dem Jahr 2011 haben 70 Prozent aller deutschen Internetnutzer ab 14 Jahren schon einmal negative Erfahrungen mit der Internet-Kriminalität gemacht. Parallel dazu steigt die Angst davor, zum Opfer zu werden. Viren und andere Schadprogramme stehen dabei für 47 Prozent der Nutzer (rund 25 Millionen Personen) an erster Stelle. Im Vorjahr waren es noch 43 Prozent. Jeder Siebte fühlte sich von einem Geschäftspartner betrogen, beispielweise bei Online-Auktionen. Die Zahl der Internetnutzer, deren Zugangsdaten z. B. zu Plattformen, Auktionshäusern oder Online-Banking ausspioniert wurden, ist von rund 3,7 Millionen im Jahr 2010 auf sieben Millionen angestiegen.

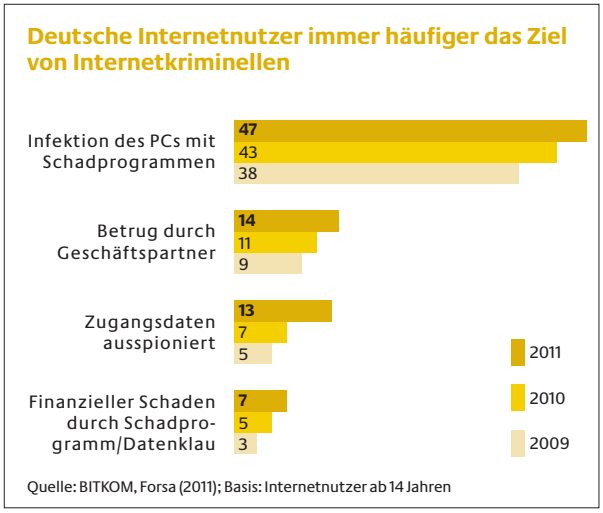


Abb. 4.3.1a: Deutschland: Erfahrungen der Internetnutzer mit Internet-Kriminalität in Prozent, 2011

Wie der Branchenverband ferner feststellt, führt die größere Angst der Verbraucher vor Angriffen nicht unmittelbar zu einem verstärkten Internet-Schutz. Jeder fünfte Deustche ist noch immer ohne Vierenschutz oder Firewall online. Dies liege aktuellen Studien zufolge daran, dass die Privatnutzer zum einen noch nicht ausreichend sensibilisiert seien oder die Komplexität der Risiken die Endanwender für die eingegangenen Sicherheitsrisiken überfordere.

Schutz der IT-Sicherheit Kritischer Infrastrukturen nimmt weiter an Bedeutung zu

Kritische Infrastrukturen haben eine besondere Bedeutung für das Gemeinwesen. Ein Ausfall kann das gesellschaftliche Wohl in Deutschland erheblich beeinträchtigen. Daher rückt die Sicherheit kritischer Infrastrukturen zunehmend in den Fokus von Wirtschaft und Politik. Die IKT-gestützten Warenströme, Logistikabläufe, Versorgungsinfrastrukturen und Verkehrsleitsysteme haben sich zu einem „zentralen Nervensystem des Landes“ entwickelt und sind verwundbar gegen Ausfälle, Angriffe und Manipulationen. Zudem werden die Sicherheitsrisiken in den branchenübergreifenden Wertschöpfungsprozessen komplexer. Auch erhöht die steigende Nutzung mobiler Internetzugänge die an die Sicherheit gestellten Anforderungen. Die zunehmende Verbreitung von „Embedded Systems“ verlangt, dass sich die IT-Sicherheit den sich wandelnden Funktionalitäten in diesen Systemen anpasst.

Die deutsche IT-Sicherheitsbranche: ein Wachstumsmarkt

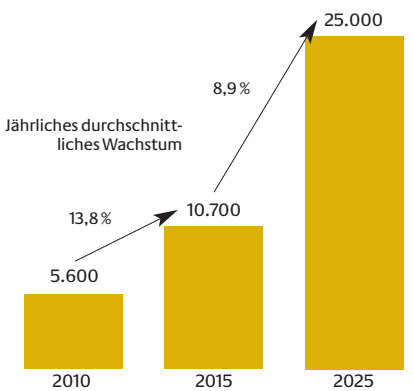
Basierend auf einer Schätzung der Analysten von IDC, die ein durchschnittliches jährliches Wachstum von 13,4 Prozent zwischen 2008 und 2012 für den globalen IT-Sicherheitsmarkt prognostizieren, wird erwartet, dass der Markt 2011 ein Volumen von 48,1 Milliarden Euro erreichen wird. Bis 2012 soll er auf 54,5 Milliarden Euro angewachsen sein. Die Wachstumsrate bei den Umsätzen mit IT-Sicherheitsdienstleistungen fallen dabei mit durchschnittlich 17,1 Prozent je Jahr stärker aus als die der IT-Sicherheitsprodukte, die durchschnittlich jährlich bei rund zehn Prozent liegt.

Wie die VDI / VDE Innovation und Technik GmbH und das Institut für Gründung und Innovation der Universität Potsdam in ihrer Studie „Technologische und wirtschaftliche

Perspektiven Deutschlands durch die Konvergenz der elektronischen Medien“ im Auftrag des Bundesministeriums für Wirtschaft und Technologie (BMWi) errechneten, ist für den deutschen Markt der IT-Sicherheitsdienstleistungen im Jahre 2025 ein Umsatzvolumen von mehr als 15 Milliarden Euro anzunehmen (ohne die Embedded Systems). Der Dienstleistungsbereich IT-Sicherheit ist ein Wachstumsträger der querschnittlich in den Konvergenzfeldern wirkenden Bereiche. Er soll mit 10 bis 15 Prozent deutlich stärker wachsen als der Hardware- bzw. Produktbereich.

Nach den Ergebnissen der folgenden Abbildung zum Markt für IT-Sicherheit, die auf Experteneinschätzungen beruht, soll der kumulierte Umsatz für den deutschen Markt für IT-Sicherheit von fünf bis sechs Milliarden Euro für IKT-Dienstleistungen, Produkte und Systeme im Jahr 2010 mit jährlichen durchschnittlichen Wachstumsraten bis 2015 auf 10,7 Milliarden Euro wachsen und sich bis 2025 um durchschnittlich jährlich 8,9 Prozent auf 25 Milliarden Euro im Jahr 2025 steigern. Der jeweils auf IKT-Anwendungen zurückzuführende Umsatzanteil wird sich den Expertenschätzungen zufolge von 70 Prozent im Jahr 2010, über 80 Prozent im Jahr 2015 auf ca. 90 Prozent im Jahr 2025 vergrößern. Die Wertschöpfung deutscher Anbieter wächst durchschnittlich jährlich von 3,5 Milliarden Euro im Jahr 2010 auf 6,6 Milliarden im Jahr 2015 und wird sich bis zum Jahr 2025 auf 18 Milliarden Euro verdreifachen.

Die Umsätze im deutschen Markt für IT-Sicherheit verfünffachen sich bis 2025



Quelle: VDI / VDE Innovation und Technik GmbH und Institut für Gründung und Innovation der Universität Potsdam im Auftrag des BMWi (2011)

Abb. 4.3.1b: Deutschland: Kumulierter Umsatz im Markt für IKT-Sicherheit in Millionen Euro, 2010 bis 2015

Die Stärken des deutschen IT-Sicherheitsmarktes

Gemäß den Ergebnissen der Studie „Die IT-Sicherheitsbranche in Deutschland“ von Booz & Company haben sich deutsche Anbieter in Marktsegmenten wie Datensicherheit sowie Identitäts- und Zugriffsverwaltung gut positioniert. „Made in Germany“ genießt allgemein und speziell im Bereich der Kryptographie einen guten Ruf. „Made in Germany“ wird im Sicherheitsbereich mit deutscher Gründlichkeit, Vertrauenswürdigkeit und hoher fachlicher Kompetenz assoziiert. Die deutschen Anbieter sind im IKT-Sicherheitsbereich gut aufgestellt. Die vielen kleinen spezialisierten Anbieter fokussieren sich insbesondere auf die klassischen Themen der Infrastruktursicherheit (VPN, Firewalls usw.).

Als besondere Stärke der deutschen Branche wird die hochwertige Ausbildung der Fachkräfte anerkannt. Das Bundesamt für Sicherheit in der Informationstechnik (BSI) ist mit seinen Zertifizierungsverfahren für Produkte, Dienstleistungen und Personen national wie international hoch angesehen. Über die Bereitstellung von technischen Vorgaben wie Schutzprofile oder technischen Richtlinien fördert das BSI die Marktentwicklung, indem die technischen Vorgaben über die Verankerung in Gesetzen, Rechtsverordnungen oder durch die internationale Normgebung für die Marktteilnehmer verbindlich gemacht werden.

Die Forschungsförderung im Bereich IKT-Sicherheit ist als Stärke zu werten. So hatte die Bundesregierung vor vier Jahren erstmals ein ressortübergreifendes Programm zur zivilen Sicherheitsforschung beschlossen. Das Bundesministerium für Bildung und Forschung (BMBF) stellte dafür bis zum Jahr 2010 zunächst 123 Millionen Euro zur Verfügung. Die Forschungsförderung ist bis zum 31.12.2013 verlängert worden und beträgt nun 222 Millionen Euro, das sind rund 74 Millionen Euro jährlich. Dabei handelt es sich nicht um ein reines Technologieprogramm. Im Schreiben der Kommission heißt es hingegen: „Deutschland sieht viel mehr in interdisziplinären Projekten mit Beteiligung der Geistes- und Sozialwissenschaften, Wissenstransfer in die Öffentlichkeit und Begleitforschung zu kritischen Fragen die Voraussetzungen für den Programmerfolg.“

Die Schwächen des deutschen IT-Sicherheitsmarktes

Die Studien „Die IT-Sicherheitsbranche in Deutschland“ und die Studie „Technologische und wirtschaftliche Perspektiven Deutschlands durch die Konvergenz der elektronischen Medien“ decken wesentliche Schwächen der deutschen Sicherheitsbranche im internationalen Wettbewerb auf.

So werden die stark fragmentierte Anbieterseite und die zu geringe Kooperationsbereitschaft der kleinen und mittleren Unternehmen insbesondere bei Clusterbildungen als nachteilig gesehen. Hinzu kommen Schwierigkeiten bei der Beschaffung von Wagniskapital sowie die generell für die IKT-Branche geltende Umsetzungslücke zwischen Innovation und Marktreife.

Bei der Herstellung der Produkte werde des Weiteren zu wenig auf eine leichte Handhabbarkeit der Produkte und auf ihre Transfermöglichkeit für einen internationalen Anwenderkreis geachtet. Bei der Produktentwicklung werden die weiteren Vermarktungschancen im Ausland oft außer Acht gelassen. Auch sei die Branche angesichts der hier fehlenden Experten nicht hinreichend in den internationalen Gremien für Standardisierung vertreten.

Darüber hinaus wirke sich der nach wie vor herrschende Fachkräftemangel im Bereich MINT auch auf die IKT-Sicherheitsbranche negativ aus. Ferner seien auch die Privatnutzer noch nicht ausreichend für die Sicherheitsthematik sensibilisiert (siehe unten).

Die Chancen des deutschen IT-Sicherheitsmarktes

Insgesamt kommen die Studien aber zu dem Schluss, dass der deutsche Markt für IT-Sicherheitsprodukte und -dienstleistungen ein Wachstumsfeld mit guten Innovierungs- und Positionierungsmöglichkeiten auf einzelwirtschaftlicher Ebene darstellt.

Treiber des Wachstums sind steigende staatliche Anforderungen an die Wahrung der nationalen IT-Sicherheit auf Grundlage der Cybersicherheitsstrategie sowie mit staatlich initiierten IT-Infrastrukturen wie De-Mail oder dem neuen Personalausweis, die wachsende Nachfrage nach Schutz von persönlichen und Unternehmensdaten sowie generell die hohen Abhängigkeiten der Sicherheitsstrategien von den Informationstechnologien. Durch die zunehmend branchenübergreifenden Wertschöpfungsprozesse steigen auch die Anforderungen an die IKT-Sicherheit. Sicherheitsaspekte werden immer stärker zum Verkaufsargument.

Maßnahmen zur Förderung der IT-Sicherheitsbranche

Vorschläge aus zusätzlichen Studien und Workshops zu den Entwicklungschancen und der Erhöhung der IT-Sicherheit:

- Erhöhte Forschungseffizienz und -fokussierung, z. B. über Sicherheitscluster, damit Deutschland als Forschungsstandort für IT-Sicherheit die Chance habe, eine weltweit führende Position zu erlangen. Dabei sei ein enges Zusmamenwirken der Unternehmen beispielsweise über den Aufbau eines Gründernetzwerks „IT-Sicherheit“ eine entscheidende Voraussetzung, um auf den Weltmärkten Führungspositionen zu erreichen.

- Die Forschungsförderung solle sich insbesondere auf die IKT-Sicherheit in Eingebettete Systemen und auf den Schutz des geistgen Eigentums und der Privatsphäre konzentrieren. Dieser sei für Innovationen im IT-Sicherheitsbereich wirksamer zu gestalten, um ungewollten Wissensabfluss und Technologietransfer zu Wettbewerbern zu verhindern.

- Der Staat sollte als Vorbild bei der Einführung innovativer IT-Sicherheitsprodukte vorangehen. In Pilotprojekten könnten neuartige Anwendungen erprobt und in der branchenübergreifenden Kooperation von Akteuren und der öffentlichen Hand erprobt werden.

- Der Staat möge finanzielle und rechtliche Anreize setzen, damit Unternehmen IT-Sicherheitsprodukte und -dienstleistungen umfänglich einsetzen.

- Die IT-Sicherheitsbranche benötige einen besseren Zugang zu den Kapitalmärkten, um ihre Innovationen zu finanzieren.

- Die Entwicklung eines umfassenden und sicheren Identitäts- und Authentifizierungsmanagements für Menschen und Objekte unter Berücksichtigung des Datenschutzes sei eine elementare Voraussetzung, um den rapiden Entwicklungen auf den IT-Sicherheitsmärkten, den Wandel der Nachfragestrukturen und den technischen Entwicklungen Rechnung zu tragen.