

# Exklusiv-Interview mit Dr. Udo Helmbrecht

## Präsident des Bundesamtes für Sicherheit in der Informationstechnik

Das Bundesamt für Sicherheit in der Informationstechnik wurde erst 1991 gegründet und ist somit eine recht junge Bundesbehörde. Probleme in der Informationstechnik sind allgemein gesprochen recht umfangreich und komplex. Welche Aufgaben hat Ihre Bundesbehörde im Besonderen und wie viele Mitarbeiter umfasst sie?



Dr. Udo Helmbrecht

**Dr. Udo Helmbrecht:** Das Bundesamt für Sicherheit in der Informationstechnik (BSI) wurde am 1. Januar 1991 gegründet und gehört zum Geschäftsbereich des Bundesministeriums des Innern. Das BSI ist eine unabhängige und neutrale Stelle für Fragen zur IT-Sicherheit in der Informationsgesellschaft. Als Behörde ist sie damit im Vergleich zu sonstigen europäischen Einrichtungen einzigartig. Derzeit sind dort rund 400 Informatiker, Physiker, Mathematiker und andere Mitarbeiter beschäftigt. Seinen Hauptsitz hat das BSI in Bonn.

Mit der rasanten Fortentwicklung der Informationstechnik entstehen in fast allen Bereichen des Alltags

neue IT-Anwendungen – und damit auch immer neue Sicherheitslücken. Je abhängiger der Mensch von der Informationstechnik wird, desto mehr stellt sich die Frage nach deren Sicherheit. Unsere Gesellschaft ist stärker als zuvor durch Computerversagen, -missbrauch oder -sabotage bedroht. Bisher kann nicht ausreichend sichergestellt werden, dass die Informationstechnik das tut, was sie soll, und nichts tut, was sie nicht soll. Weil die Probleme in der Informationstechnik so vielschichtig sind, ist auch das Aufgabenspektrum des BSI sehr komplex: Das BSI untersucht Sicherheitsrisiken bei der Anwendung der Informationstechnik und entwickelt Sicherheitsvorkehrungen. Es informiert über Risiken und Gefahren beim Einsatz der Informationstechnik und versucht Lösungen dafür zu finden. Dies beinhaltet die Prüfung und Bewertung der IT-Sicherheit von IT-Systemen, einschließlich deren Entwicklung in Kooperation mit der Industrie. Auch bei technisch sicheren Informationssystemen können Risiken und Schäden durch unzureichende Administration und Anwendung entstehen. Um diese Risiken zu minimieren beziehungsweise zu vermeiden, wendet sich das BSI an eine Vielzahl von Zielgruppen: Es berät Hersteller, Vertrieber und Anwender von Informationstechnik. Darüber hinaus analysiert es Entwicklungen und Trends in der Informationstechnik.

**Welches sind die derzeitigen aktuellen Schwerpunktthemen des BSI?**

**Dr. Udo Helmbrecht:** Ein wichtiges Aufgabengebiet des BSI ist der IT-Grundschutz, da eine mangelhaft geschützte Informationstech-

nik ein oft unterschätzter Risikofaktor ist. Für manch ein Unternehmen kann dieses Verhalten existenzbedrohend sein. Zwar gibt es sehr gute Sicherheitssysteme für die unterschiedlichen Anforderungen, diese werden aber gerade in kleinen und mittleren Unternehmen oft nur unzureichend ein- und umgesetzt. Noch immer wird IT-Sicherheit zu häufig mit „Virenschutz“ gleichgesetzt. Das Spektrum der notwendigen Maßnahmen ist jedoch viel umfangreicher.

Ein Grundschutz der IT ist allerdings schon mit verhältnismäßig geringen Mitteln zu erreichen: Die umfassende Vorlage hierzu bietet das IT-Grundschutzhandbuch des BSI. Das schon seit zehn Jahren ständig weiterentwickelte, mittlerweile rund 2.000 Seiten umfassende Standardwerk der IT-Sicherheit beschreibt detailliert Gefahren und Schutzvorkehrungen.

Um für die IT-Beauftragten und Administratoren einen leichten Einstieg in diese Informationsfülle zu schaffen, hat das BSI einen Webkurs entwickelt. In rund vier Stunden führt er den Benutzer in leicht verständlicher und kompakter Form an das Thema IT-Grundschutz heran. Durch Beispiele, Grafiken und anschauliche Texte dazu bietet das BSI das komprimierte Grundschutzhandbuch in Form eines IT-Sicherheits-Leitfadens an. Hier wird bewusst auf Details verzichtet, um einen kompakten und allgemeinverständlichen Überblick über die wichtigsten IT-Sicherheitsmaßnahmen zu schaffen. Der Leitfaden ist ideal, um eigenständig die kritischen Themen herauszugreifen. Unter Rückgriff auf das Grundschutzhandbuch können die Sicherheitsanforderungen definiert, Sicher-

heitslücken erkannt und durch Schutzvorkehrungen geschlossen werden. Der Lohn des Prozesses ist ein Unternehmen, für das IT-Sicherheitsrisiken keine große Bedeutung mehr darstellen.

Ein weiterer Aufgabenschwerpunkt des BSI ist der Bereich Internetsicherheit. Die Warnungen des BSI vor Computerviren, Internetwürmern, Trojanischen Pferden, Hoaxes und Dialern finden nicht nur in der Fachwelt inzwischen großes Gehör. Dazu bietet das BSI eine Telefon-Hotline (0 18 88/95 82-444) an sowie die Möglichkeit, per E-Mail ([antivir@bsi.bund.de](mailto:antivir@bsi.bund.de)) um Rat zu fragen.

Anfang 2001 wurde im BSI das „Computer Emergency Response Team“ für die Bundesverwaltung eingerichtet, kurz CERT-Bund. Ziel dieser zentralen Anlaufstelle ist es, präventive und reaktive Maßnahmen in Bezug auf sicherheits- und verfügbarkeitsrelevante Vorfälle in Computer-Systemen des Bundes bereitzustellen. Dazu ist CERT-Bund in der Lage, rund um die Uhr, sieben Tage die Woche auf mögliche Gefährdungen oder Angriffe zu reagieren und kurzfristig Gegenmaßnahmen zu ergreifen. Im Rahmen des Warn- und Informationsdienstes (WID) betreibt CERT-Bund Mailinglisten mit aktuellen Warnungen zu Computer-Viren, Würmern und anderen Schadprogrammen. Zusätzlich zu CERT-Bund bietet das BSI die Beratung von Behörden hinsichtlich der sicheren Internetanbindung an.

Dem BSI ist als einer unabhängigen und neutralen Einrichtung die Zertifizierung von Produkten übertragen worden. Die technische Funktionsweise von IT-Produkten (und Systemen) ist für weite Kreise der Anwendung nicht durchschaubar. Damit die Benutzer Vertrauen in die IT gewinnen können, ist jedoch gerade die Transparenz hinsichtlich der Sicherheitseigenschaften von IT-Produkten uner-

lässlich. Die Prüfung und Bewertung von IT-Produkten und -Systemen nach einheitlichen Kriterien durch unabhängige Stellen ist eine Möglichkeit, Transparenz zu schaffen. Das BSI erteilt für IT-Produkte (Systeme oder Komponenten) Sicherheitszertifikate. Die Zertifizierung eines Produktes erfolgt nach den IT-Sicherheitskriterien (Common Criteria/ITSEC) und wird auf Veranlassung des Herstellers oder eines Vertreibers durchgeführt.

[Immer wieder sind Firmen und Privatanwender Angriffen von Computerviren ausgesetzt \(Computer-Wurm Mydoom\). Zum Teil mit erheblichen wirtschaftlichen Folgen. In einem rasanten Tempo geht heute die Entwicklung hin zur globalen Informationsgesellschaft. Und mit dem gleichen Tempo steigen die Risiken, so scheint es. Wie sind solche Risiken wie Computer-Viren und Internet-Würmer zu beurteilen?](#)

Wie Sie schon richtig angemerkt haben, befinden wir uns in einer rasanten Fortentwicklung einer globalen Informationsgesellschaft, wodurch auch die Verbreitung von sog. Schadensprogrammen, wie Viren, Würmern und Tojanern dramatisch zugenommen hat. Mydoom A und B haben uns in den letzten Wochen wieder gezeigt, wie verletzlich jeder einzelne Nutzer im Internet sein kann. Bislang kennen wir über 95.000 unterschiedliche Schadensprogramme, die weltweit Kosten und Schäden verursacht haben. Allein in Deutschland ist jährlich von einem dreistelligen Millionenbetrag auszugehen. Um dieser latenten Bedrohung zu begegnen, empfehlen wir dringend den Einsatz eines stets aktuellen Virenschutzprogramms, einer Firewall und ein großes Maß an Skepsis und Aufmerksamkeit bei eingehenden E-Mails.

[Ihre Behörde hat zum Schutz „Unternehmenskritischer Infrastrukturen“, also im Bereich der Produktion, des Materials, der Logistik oder des Personals, zehn Thesen auf-](#)

[gestellt. Was ist der Inhalt und wie sollten die Thesen genutzt werden?](#)

**Dr. Udo Helmbrecht:** Das Bundesamt für Sicherheit in der Informationstechnik beschäftigt sich im Rahmen seiner bereits genannten Aufgaben mit dem Schutz von IT-abhängigen Kritischen Infrastrukturen. Kritische Infrastrukturen sind „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“. Hierzu zählen Sektoren wie Energieversorgung, Telekommunikation und IT, Behörden, Verwaltung und Justiz etc.

Vor dem Hintergrund der Definition („nachhaltig, öffentliche Sicherheit, dramatische Folgen..“) werden diese kritischen Infrastrukturen aus gesamtstaatlicher, volkswirtschaftlicher Sicht betrachtet. Um diese makroskopische Sichtweise auch auf Einzelunternehmen anzuwenden, wurde die Definition der „Unternehmenskritischen Infrastrukturen“ eingeführt. Dies „sind unverzichtbare materielle, logische oder personelle Bereiche eines Unternehmens, deren Störung oder Ausfall weitreichende und existenzbedrohende Auswirkungen für dieses haben.“ Daher hat ihr Schutz im jeweiligen Unternehmen Vorrang. Indem man die für das Unternehmen entscheidenden kritischen Geschäftsprozesse und die sie unterstützende IT und Infrastruktur identifiziert, lassen sich die nur begrenzt verfügbaren Mittel zum Schutz gezielt und angemessen einsetzen.

Um die beiden Ideenwelten Kritische Infrastrukturen und Unternehmenskritische Infrastrukturen miteinander in Bezug zu bringen, wurden Gedankenelemente übernommen und in zehn Thesen zum Schutz Unternehmenskritischer Infrastrukturen formuliert.

Diese lauten:

1. Der Schutz Unternehmenskritischer Infrastrukturen ist wegen der weitreichenden Konsequenzen Managementaufgabe.
2. Herstellung und Verbesserung der Sicherheit erfordern systematisches Vorgehen.
3. Zusammenhänge und Abhängigkeiten sind zu erkennen und zu berücksichtigen.
4. Abhängigkeiten sind zu reduzieren; unabhängige, autarke Arbeitsmodule sind anzustreben.
5. Redundanzen für identifizierte kritische Systeme sind einzuplanen.
6. Notfallpläne und Krisenkonzepte sind zu erarbeiten und zu proben.
7. Der Faktor Mensch ist zu berücksichtigen (Bequemlichkeit, Gewohnheiten, Vorlieben).
8. Der Innentäter ist noch immer als größtes Risiko zu beachten.
9. Sicherheit kann nur durch Kombination aus IT-Sicherheit und materieller Sicherheit erreicht werden.
10. Maßnahmen zum Schutz Unternehmenskritischer Infrastrukturen erfordern die Bereitstellung von entsprechenden Ressourcen (Geld, Personal, Zeit) und auch die Durchsetzung und Kontrolle durch das Management.

Ziel dieser Thesen ist es, die Diskussion zum ganzheitlichen Schutz der IT im Kontrast zur in Managementkreisen oft dominanten rein technikorientierten Sicht anzuregen. Weitere Details zu den Thesen wurden nicht ausgearbeitet, da sich diese umfangreich im Grundschutzhandbuch des BSI wiederfinden.

Täglich ärgern sich Millionen von Nutzern über den elektronischen Müll (SPAM), der in ihren Mailboxen landet. Gleichzeitig ist die elektronische Werbung für viele Firmen ein wichtiger Faktor zur

Vermarktung ihrer Produkte. Das Regeln für das Versenden von elektronischer Post soll nun gesetzlich eindeutiger und im europäischen Kontext neu verfasst werden. Reichen aber mehr Gesetze gegen SPAM aus?

**Dr. Udo Helmbrecht:** Hinsichtlich einer Bewertung von möglicherweise erforderlichen Maßnahmen auf deutscher oder europäischer Ebene zum Schutz vor sog. SPAM's muss ich Sie hier enttäuschen, da das BSI eine rein technisch ausgerichtete Behörde ist und sich mithin rechtliche Bewertungen verbieten.

Allerdings möchte ich Ihren Lesern zumindestens einige nützliche Tipps für die Abwehr von SPAM's geben. Es gibt spezielle Filterprogramme wie aber auch bei Standard-E-Mail-Programmen die Möglichkeit, gewisse Absenderadressen oder wiederkehrende und markante Textstellen zu erkennen und die Mails auszufiltern. Man sollte niemals auf eine SPAM-Mail antworten. Häufig sind Schaltflächen vorhanden über die man angeblich diese Mail abbestellen kann (oder ähnliches). Dies führt aber nicht zum Ziel. Im Gegenteil, hierdurch wird nur die Existenz der Adresse verifiziert. SPAM-E-Mail sollte einfach (ungelesen) gelöscht werden.

Sicherheit in der Informationstechnik ist eine europäische, im Grunde ja weltweite Aufgabe. Welche Zusammenarbeit pflegt das BSI mit anderen Europäischen Behörden, die ähnliche Aufgaben haben, speziell auch mit der EU in Brüssel?

**Dr. Udo Helmbrecht:** Die weltweite Vernetzung der Kommunikations- und Informationssysteme zwingt zu international abgestimmtem Handeln, gerade im Bereich der IT-Sicherheit. Deshalb engagiert sich das BSI aktiv in internationalen Gremien, z.B. der EU oder NATO. Durch die Mitarbeit sollen die Entwicklungen der Informationssicherheit frühzeitig er-

kannt und damit Sicherheitsrisiken entgegengewirkt werden. Die Arbeit des BSI hat Gewicht: Deutschland gehört auf dem Gebiet der IT-Sicherheit zu den führenden Staaten; ausgewiesen durch eine jahrzehntelange Erfahrung im staatlichen Bereich, beachtliche Forschungsergebnisse und begründet durch die Leistungsfähigkeit der einschlägigen Industrie. Dieses Potenzial zu fördern – und den Einfluss weiter auszubauen – ist ein vordringliches Ziel der internationalen Zusammenarbeit.

Ein weiterer Aspekt liegt in der Förderung der Marktchancen deutscher Hersteller. Neben der traditionell intensiven Beteiligung des BSI in Gremien und Projekten der NATO gewinnt das Engagement im Zusammenhang mit der europäischen Integration zunehmend an Bedeutung. Das BSI ist die akkreditierte nationale INFOSEC-Behörde beim Generalsekretariat des Ministerrates der EU. Es unterstützt die Europäische Union bei der Gestaltung und der Umsetzung der Sicherheitsvorschriften für klassifizierte Informationen. Der Bedarf ergibt sich aus der Aufgabe des Generalsekretariats, die gemeinsame Außen- und Sicherheitspolitik der EU zu koordinieren. Die Mitarbeit erfolgt in vielfältiger Weise: Beratungsleistungen für neue Netzwerke, Projekte und Serviceleistungen, Angebot und Evaluierung von Kryptogeräten und Akkreditierung von Systemen. Die Erfahrungen in der Zusammenarbeit mit EU und NATO eröffnen im Rahmen der Erweiterung der europäischen Union und des nordatlantischen Bündnisses eine Reihe von fruchtbaren, bilateralen Kontakten. Sie begünstigen die Verbreitung der BSI-Sicherheitsphilosophie und erschließen Märkte für die durch das BSI geförderten Sicherheitsprodukte.

**Das Interview führte Jürgen Klocke**

**Kontakt BSI: [www.bsi.bund.de](http://www.bsi.bund.de)**