Bundesamt
für Sicherheit in der
Informationstechnik

Mit Sicherheit

BSI-Magazin 2016/01

25 Jahre BSI

Mit Transparenz mehr Sicherheit

Liebe Leserinnen und Leser,

in dieser Ausgabe des BSI-Magazins blicken wir zurück auf ein Viertel-jahrhundert deutsche IT-Sicherheits-geschichte, denn das Bundesamt für Sicherheit in der Informationstechnik feiert in diesem Jahr sein 25-jähriges Bestehen. Bereits in den 1990er-Jahren, den „frühen Jahren der IT-Sicherheit", war die Bedrohung durch Computerviren ein Thema des BSI. Damals hatten Computerviren und -würmer noch einen exotischen Charakter, es gab lediglich ein bis zwei neue Viren im Monat. Das BSI trat dieser ersten Bedrohungslage mit Antivirus-Disketten entgegen – heute kaum mehr vorstellbar.

Durch den „I-Love-You-Virus", der Anfang der 2000er-Jahre schätzungsweise 10 Milliarden US-Dollar Schaden anrichtete, rückte das bisherige „Nischenthema" Cyber-Sicherheit erstmals in das öffentliche Bewusstsein. Der „Millenium-Bug" bzw. das „Jahr-2000-Problem" beschäftigte nicht nur deutsche Computerbesitzer, sondern sorgte auch in der Bundesverwaltung für erheblichen Aufwand und führte zu massiven Vorbereitungen auf deren möglichen Ausfall. Die Erfahrungen mit dem Schadprogramm Stuxnet im Jahre 2010 zeigen, dass auch wichtige industrielle Infrastrukturbereiche von gezielten IT-Angriffen nicht mehr verschont bleiben. Stuxnet war erstmalig dazu in der Lage, Prozesssteuerungssysteme von Industrieanlagen anzugreifen. Die Programme Duqu und Flame sorgten 2012 aufgrund ihrer hohen Funktionalität und Komplexität für eine weitergehende Sensibilisierung im Bereich „Cyber-Sicherheit".

Es haben sich daher seit der Gründung des BSI im Januar 1991 nicht nur die Gefährdungslage und die technischen Mittel zur Abwehr von Cyber-Angriffen fundamental verändert. Auch die Gesetzeslage, auf der die Aufgaben, Rechte und Pflichten des Amtes basieren, hat sich immer wieder den aktuellen Entwicklungen angepasst und dem BSI adäquate Mittel zur präventiven Gefahrenabwehr an die Hand gegeben.

Auch deswegen ist das BSI heute gut aufgestellt, um zum Beispiel bei Angriffen auf die Bundesverwaltung schnelle Hilfe zu leisten. Das ist wichtig, denn die Bewältigung eines Cyber-Spionageangriffs ist für die betroffenen Institutionen kein Tagesgeschäft und kann schnell mehrere hundert Personentage umfassen. Was passiert, wenn die Prävention doch einmal versagt, und wie solche Vorfälle im BSI gehandhabt werden, lesen Sie in dieser Ausgabe.

Europaweit werden die Weichen für das Internet der Dinge gestellt. Die globale Vernetzung der IT-Systeme sorgt dafür, dass sich Vorfälle in Informationsinfrastrukturen anderer Länder auch mittelbar auf Deutschland auswirken können. Daher blicken wir auch nach vorne in einen Zukunftsmarkt der Cyber-Sicherheit: das

Arne Schönbohm,
Präsident des Bundesamts für Sicherheit in der Informationstechnik

automatisierte Fahren. 2016 wird der Einsatz von Assistenzsystemen, die eigenständig das Fahrzeug lenken, die Spur wechseln und im Notfall auch das Auto abbremsen, erstmals erlaubt sein. Mit den dafür nötigen neuen Kommunikationsmöglichkeiten werden die Fahrzeuge zur Außenwelt hin „geöffnet" und damit auch einem möglichen Missbrauch durch potentielle Angreifer ausgesetzt. Zur Absicherung der Kommunikation zwischen Fahrzeugen und Verkehrsleitzentralen arbeitet das BSI bereits heute an der Entwicklung eines entsprechenden IT-Sicherheitskonzepts, das wir Ihnen im aktuellen BSI-Magazin vorstellen möchten.

Ich wünsche Ihnen eine anregende Lektüre und viele interessante Einblicke in bekannte und neue Themen der Cyber-Sicherheit.

Bonn, im März 2016

Arne Schönbohm,
Präsident des Bundesamts für Sicherheit in der Informationstechnik

AKTUELLES

CYBER-SICHERHEIT

DIGITALE GESELLSCHAFT

25 JAHRE BSI

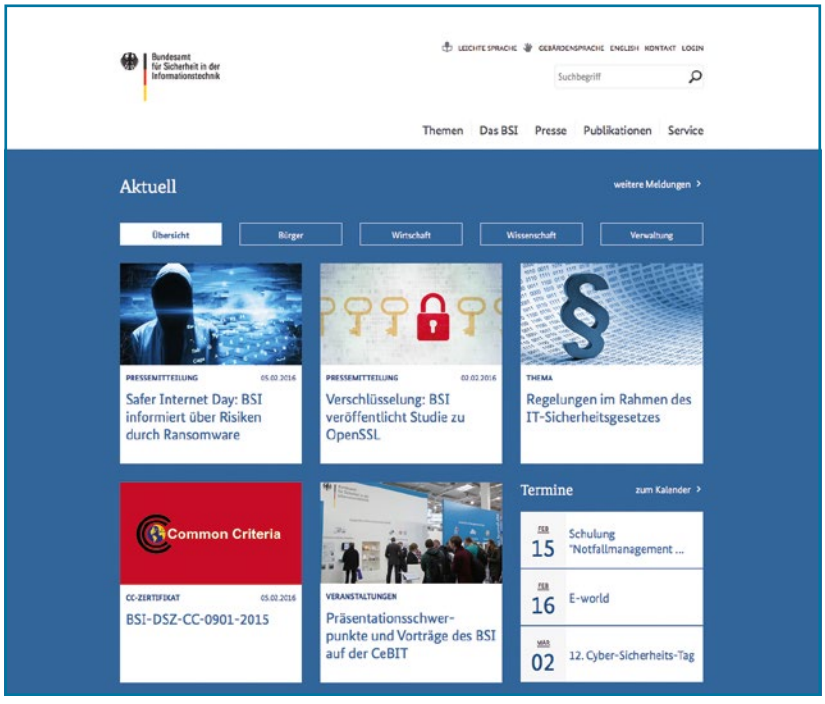
IT-SICHERHEIT IN DER PRAXIS

DAS BSI UND SEINE AUFGABEN

Kurz notiert

BSI-Präsident Hange in den Ruhestand verabschiedet

Bundesinnenminister Dr. Thomas de Maizière hat am 11. Dezember 2015 in Bonn den bisherigen Präsidenten des BSI Michael Hange in den Ruhestand verabschiedet. Hange leitete die Bonner Behörde seit Oktober 2009. Nach Erreichen der Altersgrenze schied er zum 30. November 2015 aus dem aktiven Dienst aus.



IT-Lagebericht 2015 in Berlin vorgestellt

Bundesinnenminister Dr. Thomas de Maizière und der damalige BSI-Präsident Michael Hange stellten am 19. November 2015 in Berlin den Bericht zur Lage der IT-Sicherheit in Deutschland vor. Der Bericht beschreibt und analysiert die aktuelle IT-Sicherheitslage, die Ursachen von Cyber-Angriffen sowie die verwendeten Angriffsmittel und -methoden. Daraus abgeleitet thematisiert er Lösungsansätze zur Verbesserung der IT-Sicherheit in Deutschland. Der Lagebericht steht unter www.bsi.bund.de/Lageberichte zur Verfügung.

Relaunch: BSI-Webseiten in neuem Design

Das BSI hat seine Webseiten umfangreich überarbeitet: Die Seiten wirken aufgeräumter, das Design ist moderner, die Benutzerführung wurde verbessert und die Seiten stärker den Bedürfnissen mobiler Geräte angepasst. Unter www.bsi.bund.de, www.bsi-fuer-buerger.de und www.allianz-fuer-cybersicherheit.de finden sich die Internetangebote des BSI.

Wirtschaftsschutz: Telekom für Lauschabwehr zertifiziert

Das BSI hat die Deutsche Telekom als erste Institution als IT-Sicherheitsdienstleister auf dem Gebiet „Lauschabwehr im Bereich der Wirtschaft“ zertifiziert. Die Deutsche Telekom hat nachgewiesen, dass bestimmte Mindest-Qualitätsstandards bei der Planung, Durchführung und Nachbereitung von Lauschabwehrprüfungen eingehalten werden. Zudem verfügt das Unternehmen über Kompetenz in der Anwendung eines breit gefächerten Spektrums an Prüfverfahren. Die unabhängige BSI-Zertifizierung soll es Unternehmen vereinfachen, qualifizierte Dienstleister im Bereich der Lauschabwehr zu finden.

IT-Sicherheitsgesetz: Entwurf für KRITIS-Verordnung liegt vor

Das Bundesministerium des Innern hat im Februar 2016 den Referentenentwurf einer Verordnung zur Bestimmung Kritischer Infrastrukturen (BSI-KritisV) zur Stellungnahme an die Länder und Verbände übermittelt. Die Verordnung ergänzt das IT-Sicherheitsgesetz. Dieses regelt unter anderem, dass Betreiber Kritischer Infrastrukturen zur Umsetzung von Mindeststandards verpflichtet und IT-Sicherheitsvorfällen an das BSI gemeldet werden müssen. Mit der Verordnung können Betreiber Kritischer Infrastrukturen anhand messbarer und nachvollziehbarer Kriterien prüfen, ob sie unter den Regelungsbereich des IT-Sicherheitsgesetzes fallen.

CSCG: Nachwuchshacker gesucht

Um die digitale Zukunft Deutschlands sicherer zu gestalten, tragen das Institut für Internet-Sicherheit if(is) und TeleTrusT Bundesverband IT-Sicherheit e.V., die „Cyber Security Challenge Germany – CSCG“ (www.cscg.de) aus. Gesucht werden die besten Nachwuchshacker Deutschlands zwischen 14 und 30 Jahren, die ab Mai 2016 Online-Challenges lösen. Wer im Finale im September in Berlin seine Fähigkeiten unter Beweis stellt, qualifiziert sich damit für die European Cyber Security Challenge (ECSC).

Analyse: TrueCrypt weiterhin zur Verschlüsselung geeignet

Im Auftrag des BSI untersuchte das Fraunhofer-Institut für Sichere Informationstechnologie SIT die Verschlüsselungssoftware TrueCrypt auf Sicherheitslücken. Ergebnis: TrueCrypt eignet sich weiterhin für die Verschlüsselung von Daten auf Datenträgern. Die vollständige TrueCrypt-Analyse steht unter www.bsi.bund.de/Studien zur Verfügung.

European Cyber Security Month

Im Oktober 2016 wird das BSI erneut am European Cyber Security Month (ECSM, https://cybersecuritymonth.eu/) teilnehmen. Dabei übernimmt das BSI die Rolle der Koordinierungsstelle. Der europaweite Aktionsmonat findet jährlich unter Federführung der europäischen IT-Sicherheitsbehörde ENISA (European Union Agency for Network and Information,Security) statt, mit dem Ziel Bürgerinnen und Bürger sowie Unternehmen und Organisationen für das Thema Cyber-Sicherheit zu sensibilisieren. Im vergangenen Jahr definierte das BSI hierzu vier Leitthemen, die während des ECSM erfolgreich aufbereitet und gespielt wurden.

EUROPEAN CYBER SECURITY MONTH

„In Sicherheitsfragen darf es keine Kompromisse geben“

Interview mit Guus Dekkers, CIO Airbus und Airbus Group

Seit 2008 ist der Holländer Guus Dekkers IT-Chef bei der Airbus Group und hat seitdem viel Lob, vor allem für die Einbindung verschiedenster Innovationen in die Unternehmens-IT, bekommen. Nichtsdestotrotz stehen Hightech-Unternehmen, was Airbus Group zweifelsohne ist, ganz besonders im Fokus von Cyber-Angreifern. Dass Cyber-Abwehr ein ganz zentraler Bestandteil der Unternehmensaktivitäten ist, erklärt er im Interview.

Inwieweit hat sich denn die Cyber-Gefahrenlage für Airbus Group in den letzten Jahren verändert?

Die Gefahrenlage hat sich in zweierlei Hinsichten geändert. Zum einen hat sich der Fokus der Cyber-Bedrohungen verlagert – weg von der Kerngesellschaft, hin zu den kleineren Beteiligungsgesellschaften oder unserer Supply-Chain. Diese Entwicklung ist nachvollziehbar, da wir in den vergangenen Jahren umfangreiche Investitionen getätigt haben, um unsere Kernprozesse bestmöglich abzusichern. Wenn der Vordereingang deutlich besser geschützt ist, richtet sich nun mal der Blick der Cyber-Angreifer verstärkt auf die Hintertür – dessen sind wir uns bewusst.

Die zweite Entwicklung, die wir beobachten, ist, dass Attacken auf die Angriffsziele deutlich individueller abgestimmt sind. Beispielsweise wird Malware gezielt für ein einmaliges spezielles Einsatzszenario entworfen und dafür genutzt, um sich Zutritt zu verschaffen. Der Mangel an prädiktiven Prüfungsalgorithmen macht die Identifizierung solcher Einbruchsversuche daher immer schwieriger. Insbesondere kleinere Unternehmen haben nachvollziehbarerweise Schwierigkeiten, solchen unüblichen Angriffsszenarien auf die Spur zu kommen.

Welcher Arten von Cyber-Angriffen werden aus Ihrer Sicht in den kommenden Jahren auf Unternehmen zukommen?

Vor einigen Jahren waren die vordergründigen Herausforderungen eines IT-Verantwortlichen im Unternehmen vor allem der Schutz des intellektuellen Eigentums und das Unterbinden von finanziellem Betrug. Mittlerweile liegt jedoch das Hauptaugenmerk auf der Wertschöpfungskette der Unternehmen. In der Verantwortung der IT-Abteilungen

Kurzprofil Guus Dekkers

Guus Dekkers ist seit 2008 CIO bei der Airbus Group und CIO der Unternehmens-Division Airbus. In dieser Position zeichnet er verantwortlich für alle in der Airbus Group weltweit eingesetzten IT-Systeme und -Architekturen. Vor seiner Tätigkeit für Airbus arbeitete Dekkers insgesamt 18 Jahre in namhaften Unternehmen der Automotive-Branche wie Volkswagen, Johnson Controls und Siemens sowie Continental. Während dieser Zeit bekleidete er verschiedene IT-Posten und stieg so schrittweise zum CIO auf. Dekkers hat Erfahrung in unterschiedlichen Ländern gesammelt, darunter Deutschland, Frankreich und Mexiko. Die Fachzeitschrift COMPUTERWOCHE wählte Dekkers 2013 zum „CIO des Jahres“. Der Niederländer hat einen Abschluss in Informatik der Radboud Universität in Nijmegen/Niederlande und einen MBA (Master of Business Administration) der Rotterdam School of Management. Dekkers lebt mit seiner Familie in Toulouse in Frankreich.

Wir haben Spezialisten-Teams aufgebaut mit dem Ziel, unsere Produkte schon im Entwicklungsprozess „cyber-safe“ zu denken und zu gestalten.

liegt es, Bedrohungen abzuwenden, die die Wertschöpfungsprozesse des Unternehmens beeinträchtigen können. Denn Software ist Bestandteil der Mehrzahl unserer Produkte. Viele sind Teil einer vernetzten Ökosphäre. Die intelligente Vernetzung von Geräten und Maschinen, die unter dem Begriff „Internet der Dinge“ zusammengefasst wird, bringt nicht nur besondere Anforderungen in Sachen Absicherung und Produkthaftung mit sich. Ein Ausfall, ausgelöst durch einen Cyber-Angriff, kann maßgeblich die Reputation und das Wachstum eines Unternehmens beeinflussen. Was so ein Vorfall für Airbus Group bedeuten würde, kann man sich leicht ausmalen.

Resultat ist, dass unsere Aufgaben im Bereich IT-Sicherheit nicht nur im Umfeld der klassischen Informations- und Kommunikationstechnik deutlich gestiegen sind. In den vergangenen Jahren haben sich die Aufwendungen verdreifacht, sodass wir nunmehr einen größeren zweistelligen Millionenbetrag pro Jahr in unsere IT-Sicherheit investieren. Unser Ziel ist es auch, sicherzustellen, dass unsere Produkte schon im Design-Prozess „cyber-safe“ gestaltet und realisiert werden. Hierfür haben wir dedizierte Teams aufgebaut.

Über die Airbus Group

Die Airbus Group ist ein weltweit führendes Unternehmen im Bereich Luft- und Raumfahrt sowie den dazugehörigen Dienstleistungen. Der Umsatz betrug € 60,7 Mrd. im Jahr 2014, die Anzahl der Mitarbeiter rund 138.600. Zum Konzern gehören die Divisionen Airbus, Airbus Defence and Space sowie Airbus Helicopters.

Ein Blick in die Schaltzentrale des Airbus A350 XWB – das Cockpit vereint Hightech, Komfort und höchste Sicherheit.

IT-Sicherheit geht oft auch mit einem Einschnitt im Komfort des gelernten Nutzungsverhaltens einher. Wie gehen Sie bei Airbus Group dieses Spannungsfeld für Ihre Mitarbeiter an?

Unerfreulicherweise hilft uns die Tatsache, dass zwischenzeitlich viele Mitarbeiter negative Erfahrungen mit Cyber-Angriffen in ihrem persönlichen Umfeld machen mussten. Hier fällt es uns leichter, unsere Mitarbeiter für bestimmte Verhaltensweisen zu sensibilisieren. Jedoch bleibt für viele Menschen die Gefahrenlage sehr abstrakt und im konkreten Fall schwer einzuschätzen – frei nach dem Motto: „Was man nicht sieht, kann auch keinen Schaden anrichten." Hier setzen wir mit breiten und kontinuierlichen Aufklärungskampagnen an. Dies sind E-Learning-Angebote, unterhaltsame Sensibilisierungsvideos, aber auch Seminare mit Live-Hacking-Sessions, die übrigens sehr gut besucht sind. Nichtsdestotrotz ist das Spannungsfeld zwischen erwartetem Nutzungskomfort, neuen Funktionalitäten, dem verfügbaren Finanzrahmen und den erforderlichen Sicherheitsmaßnahmen sehr komplex. Oft wird der Bedienungskomfort des Einzelnen über wichtige Grundlagen der IT-Sicherheit gestellt und Erwartungen formuliert, die den unbeschränkten Möglichkeiten aus dem privaten Umfeld entsprechen. Hier kommt es leider zu Unverständnis, wenn bestimmten Handlungsweisen aufgrund von Bedenken bezüglich der IT-Sicherheit abgelehnt werden müssen.

Stichwort Messung des Beitrages von IT-Sicherheit zur Unternehmenswertschöpfung: Wie messen und argumentieren Sie den Nutzen notwendiger Ausgaben in die Sicherheit der Unternehmens-IT?

Ich vergleiche die Investitionen in IT-Sicherheit im Unternehmen gerne mit den Beiträgen einer Krankenversicherung. Wenn man sich eine bessere Krankenversicherung aussucht und bereit, ist die damit verbundenen Kosten langfristig zu tragen, hat man zwar keine Garantie, dass man gesund bleibt. Dennoch hat man auf jeden Fall Sorge getragen, dass man die bestmöglichen Vorkehrungen getroffen hat.
Mit herkömmlichen Wirtschaftskriterien wird sich nie konkret beurteilen lassen, ob alle Investitionen richtig waren. Die Unternehmensführung ist sich jedoch der branchenspezifischen, hohen Risiken bewusst, sollte man nachlässig mit dem Thema IT-Sicherheit umgehen, und wird hier keinerlei Kompromisse eingehen. Aus diesem Grund existiert bei uns seit einigen Jahren ein konzernweites IT-Security-Programm, das unmittelbar an die Geschäftsleitung berichtet und entsprechend mit finanziellen Mitteln ausgestattet ist. Diese Vorgehensweise kann sich jedoch durchaus von der anderen Industrien unterscheiden.

Aber sind Sie in der Lage, durch Indikatoren nachzuweisen, wie viel besser Sie die Gefahrenlage einschätzen können?

Durchaus. Wir beobachten in unserem Cyber-Monitoring-Center 24 Stunden und 7 Tage die Woche die aktuelle Gefahrenlage. Somit stehen uns kontinuierlich Auswertungen zur Verfügung. Jeden Monat entdecken wir im Schnitt 180 sogenannte Day-0 Exploits, sprich Malware, die man mit üblichen Methoden nicht ohne Weiteres hätte entdecken und lokalisieren können. Des Weiteren informieren wir im Schnitt ca. 40 Webseiten-Betreiber monatlich, dass deren Webseiten für Cyber-Angriffe gekapert und missbraucht werden. Ein Großteil der Betroffenen sind für derartige Hinweise zwar sehr dankbar, dennoch ist meist die Überraschung darüber sehr groß.

Wenn Sie sich etwas wünschen können, welche Rolle sollten Branchenverbände und öffentliche Institutionen beim Thema IT-Sicherheit in Zukunft noch stärker einnehmen?

Ich mache mir hier eher Sorgen um den deutschen Mittelstand als um größere Unternehmen. Die Konzerne sind durchaus in der Lage, die Bedrohungslage zu beobachten, richtig einzuschätzen und die notwendigen Maßnahmen für sich voranzutreiben. Dies fällt den deutschen KMUs (kleine und mittelständische Unternehmen) deutlich schwerer. Zieht man noch in Betracht, dass kleine und mittelständische Unternehmen die wesentlichen Innovatoren und der Motor der deutschen Ökonomie sind, müssen Wege gefunden werden, diese in Sachen IT-Sicherheit noch stärker zu unterstützen. Dies sehe ich auch als Aufgabe von Branchenverbänden und öffentlichen Institutionen.
Airbus Group hat im Laufe der letzten Jahren gelernt, wie viele Vorteile die Zusammenarbeit in Sachen „Situational Awareness" bei der Interpretation der Gefahrenlage allen Beteiligten bringt. Fußt die Zusammenarbeit auf einer guten Vertrauensbasis, helfen der regelmäßige Austausch zu „Best Practices" und die gemeinschaftliche Auseinandersetzung mit aktuellen Bedrohungsszenarien. So können die knappen finanziellen Mittel so effizient wie möglich eingesetzt werden.

Wie sieht das Ihrer Meinung nach in der Zukunft aus?

Wir sollten uns alle klarmachen, dass das Thema Cyber-Kriminalität lange nicht vorbei oder nachhaltig eingedämmt ist. Die momentan sichtbaren IT-Security-Themen stellen erst den Anfang dar. Sowohl die sich schlagartig entwickelnde Vernetzung der Industrie, als auch die immer rasantere Zunahme und Abhängigkeit von IT-Lösungen werden dafür sorgen, dass IT-Sicherheit einen Großteil unserer Tagesordnung mitbeherrschen wird. Ich sehe es daher als Pflicht jeder Geschäftsleitung bzw. jedes IT-Verantwortlichen, sich rechtzeitig damit zu befassen. ●

Wenn die Prävention nicht geholfen hat

Voraussetzungen für die erfolgreiche Bewältigung von Cyber-Spionagefällen

Derzeit überbieten sich IT-Sicherheitsfirmen mit der Veröffentlichung von neuen Cyberspionage-Angriffskampagnen. Oftmals fokussieren sie dabei auf Aspekte der verwendeten Schadsoftware und fassen die Betroffenheit von Institutionen in einem Halbsatz zusammen. Was dabei vergessen wird: Diese Veröffentlichungen beziehen sich meistens auf Vorfälle mit Analyse-Aufwänden von jeweils mehreren Hunderten von Personentagen. Für die Betroffenen ist die erfolgreiche Bewältigung eines Vorfalls kein Tagesgeschäft. Dieser Artikel stellt die Rahmenbedingungen für die nachhaltige Bereinigung eines solchen Vorfalls dar.

Die Kontaktaufnahme

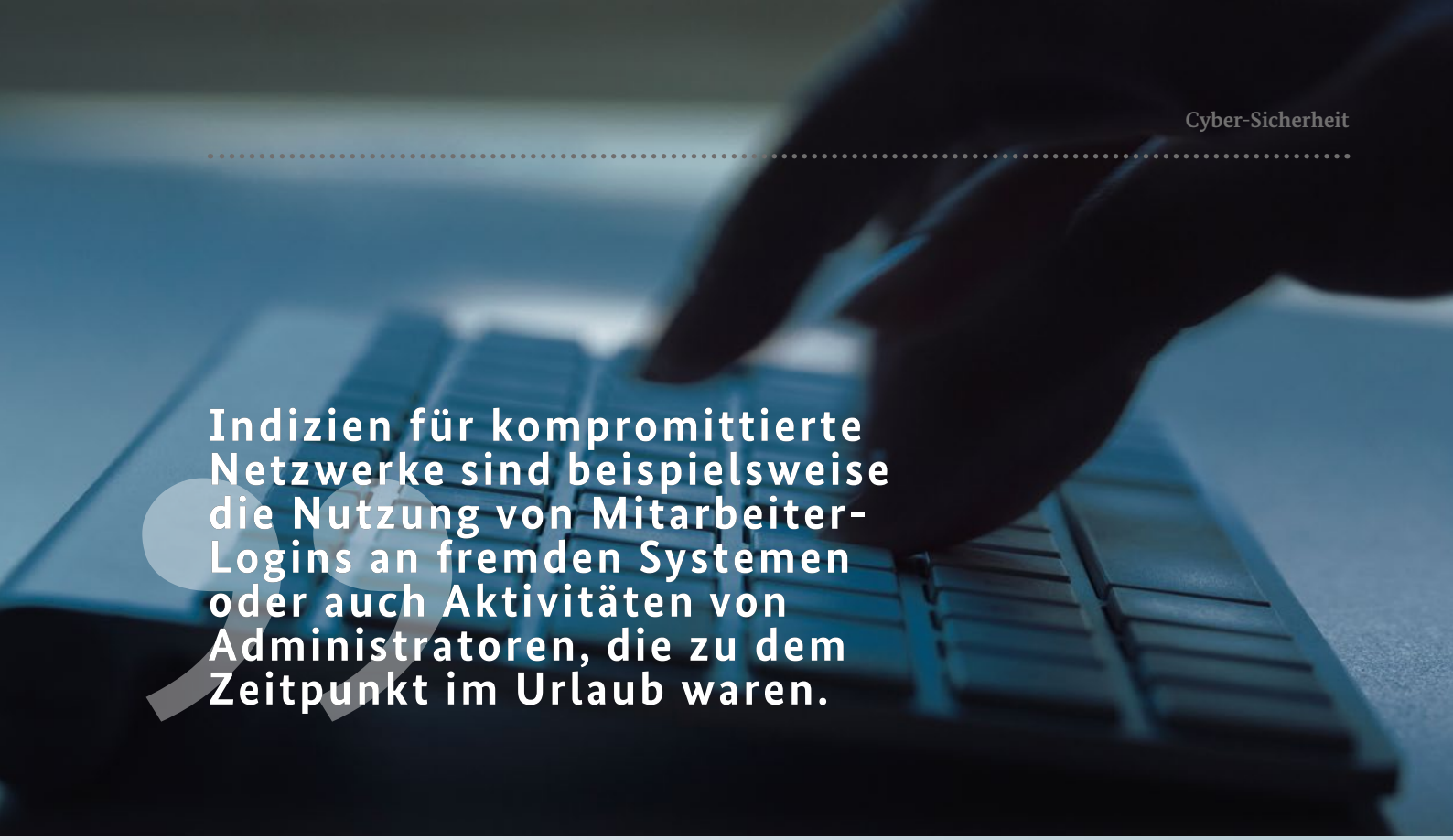
Die Erfahrung zeigt, dass ernste Netzwerkkompromittierungen in den meisten Fällen von Dritten an die betroffene Institution gemeldet werden. Das liegt daran, dass viele Institutionen nur Schutzmechanismen gegen initiale Angriffsvektoren besitzen. Wenn diese unterlaufen wurden, haben die Betroffenen meistens keine Mittel zur Verfügung, um die Aktivität der Täter im eigenen Netz zu erkennen.
Daher wird ein Großteil der massiven Netzwerkkompromittierungen erst aufgedeckt, wenn externe Stellen große Angriffskampagnen und in diesem Rahmen Kontrollserver der Täter untersuchen. Auf diesen Kontrollservern verbinden sich die Schadprogramme, die im Netzwerk der Betroffenen installiert sind. Durch die Auswertung dieser Verbindungen können Analysten oder Ermittler auf die betroffene Institution schließen und sie informieren.

Oftmals kontaktieren Analysten Betroffene in Deutschland nicht direkt, sondern wenden sich an das BSI als zentralen Ansprechpartner. Dem BSI obliegt es, in Absprache mit den anderen Sicherheitsbehörden die Vorfälle zu bewerten und die Betroffenen zu informieren.

Wenn das BSI Informationen über Verbindungen zu Kontrollservern erhält, sind das im Wesentlichen Zeitstempel, die IP-Adressen der Betroffenen und die Adresse des Kontrollservers. Oftmals wird auch die verwendete Schadsoftware genannt. Anders als normale Schadsoftware, wie zum Beispiel Banking-Trojaner, sind Cyber-Spionageprogramme darauf ausgelegt, den Tätern den Einstieg in das interne Netzwerk zu ermöglichen und das sogenannte Lateral Movement zu unterstützen. Das heißt, die Täter hangeln sich von einem internen System zum nächsten, bis sie an genau die Daten gelangt sind, für die sie sich interessieren. Anhand der Informationen, die das BSI initial erhält, ist es in den meisten Fällen nicht möglich abzuschätzen, wie viele Rechner im Netzwerk der betroffenen Institution infiziert sind und wie tief die Täter bereits in interne Bereiche vorgedrungen sind. Auch für die Mitarbeiter aus dem betroffenen IT-Betrieb ist die Untersuchung, ob und wie viele Rechner betroffen sind, eine Herausforderung. Auch wenn dies sehr aufwendig ist, liegt es im eigenen Interesse der betroffenen Institution, eine solche eigene Untersuchung vorzunehmen.
Bei der Kontaktaufnahme durch das BSI gilt es, den Ansprechpartnern zu vermitteln, dass es bei Angriffen von professionellen Cyber-Spionage-Gruppen nicht damit getan ist, die Rechner zu bereinigen, welche die Verbindungen zum Kontrollserver initiiert haben. Stattdessen muss untersucht werden, wie weit die Täter das Netzwerk bereits kompromittiert haben.

Zu diesem Zweck müssen zentrale Logdaten aufwändig ausgewertet werden. Die Anhaltspunkte für die Aktivitäten der Täter sind oft indirekt. Beispiele dafür sind Aktivitäten von Administratoren, die zum Zeitpunkt der Aktivität im Urlaub waren, das Kopieren von gestohlenen Daten und übergelaufene Festplatten oder Logins von Nutzern auf fremden Systemen. Häufig liegen die benötigten Logdaten weder lang genug, noch detailliert genug vor, und sowohl Personalrat als auch Datenschutzbeauftragte sehen oft keinen hinreichenden Anfangsverdacht, um die Logdaten freizugeben. Zudem ist bei der betroffenen Institution das nötige Know-how meist nicht vorhanden, um Logdaten auf solche Auffälligkeiten zu untersuchen.
Da auch das BSI über begrenzte Ressourcen verfügt, rät das BSI gegebenenfalls, externe Dienstleister zu beauftragen.

Ein weiterer Punkt, der unmittelbar nach der Kontaktaufnahme geklärt werden muss, betrifft die interne Kommunikation. Üblicherweise werden derartige Vorfälle in der betroffenen Institution zunächst geheimgehalten



Indizien für kompromittierte Netzwerke sind beispielsweise die Nutzung von Mitarbeiter-Logins an fremden Systemen oder auch Aktivitäten von Administratoren, die zu dem Zeitpunkt im Urlaub waren.

und nur von wenigen Eingeweihten bearbeitet. Es lässt sich nie ganz vermeiden, dass Nichtbeteiligte misstrauisch werden. Spätestens wenn externe Dienstleister in der IT-Abteilung auftauchen, das IT-Personal befragen und Rechner einziehen, erweitert sich der Kreis der Involvierten. Gegebenenfalls kann eine Cover-Story entwickelt werden.

Wie die betroffene Institution mit dem Vorfall umgeht, lässt sich von externer Seite nur begrenzt beeinflussen. Maßgeblich entscheidend ist dabei die Unternehmenskultur, wie die Transparenz bei der internen Kommunikation oder das Renommee, das dem eigenen IT-Betrieb zugemessen wird.

Die Analyse

Typischerweise wird die Analyse von externen Dienstleistern oder Analysten des BSI durchgeführt. Die erste Herausforderung ist stets, bei der betroffenen Institution hinsichtlich der technischen Analyse arbeitsfähig zu werden. Denn die Analysten können nicht im möglicherweise kompromittierten Netzwerk arbeiten, das heißt, sie brauchen eine eigene Infrastruktur. Dies umfasst Analyse-Arbeitsplätze, Internetzugang, Server zum Ablegen von Analyse-Ergebnissen und riesigen Speicherplatz für die Kopien von zu untersuchenden Festplatten sowie schnelle Server zum Analysieren von Gigabytes an Logdaten. So banal es klingt, die vorbereitenden Maßnahmen dauern einige Tage und bedürfen zudem der Abstimmung mit der betroffenen Institution. Forderungen nach Nachteinsätzen und stündlichen Ergebnissen bei Netzwerkkompromittierungen gehen an der Realität vorbei.

Oft befürchten IT-Mitarbeiter und zuständige Vorgesetzte in der betroffenen Institution, als Sündenbock ausgemacht zu werden. Dies führt mitunter zu Versuchen, vermeintliche eigene Fehler zu vertuschen, indem nachträglich vergessene Sicherheitsupdates eingespielt oder zusätzliche Sicherheitsmaßnahmen etabliert werden, die Spuren der Täter überschreiben. Zudem untergräbt die Angst vor Schuldzuweisungen ein offenes und konstruktives Arbeitsklima, in dem Administratoren ihre notwendige Kenntnis des Netzwerks einbringen können. Daher stellt das BSI stets klar, dass es bei der Untersuchung nicht darum geht, Schuldige zu identifizieren, sondern die Netzwerkkompromittierung zu beheben und zukünftige Angriffe zu erschweren.

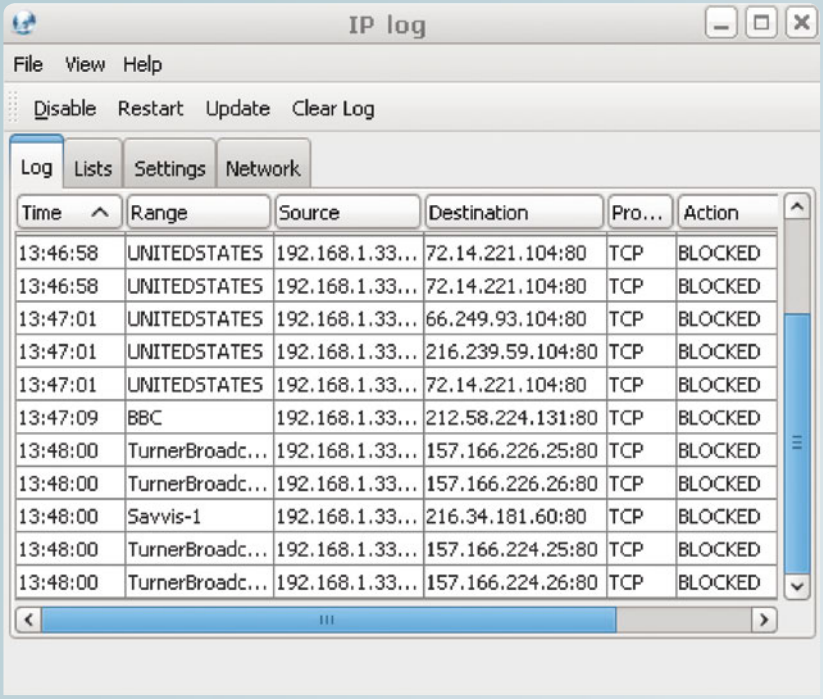
Eine sofortige bloße Bereinigung der infizierten Systeme ist nicht zielführend, da die Täter eventuell bereits tief ins interne Netzwerk vorgedrungen sind und weitere (noch nicht identifizierte) Systeme oder Zugangsdaten kompromittiert haben. Daher ist das Ziel der Analyse, das Ausmaß des Vorfalls zu bestimmen und das Vorgehen der Täter zu verstehen. Dabei geht man iterativ vor. Die bereits bekannten technischen Details werden zu Signaturen verarbeitet, um im Netzwerk nach weiteren Spuren der Täter zu suchen. Werden dabei weitere Systeme oder Artefakte gefunden, werden diese untersucht, um neue Indikatoren zu erstellen. Mit diesen kann dann erneut das Netzwerk durchsucht werden. Wenn sich nach solch einer Schleife kein neuer Erkenntnisgewinn einstellt, kann dies als Hinweis genommen werden, dass die Analyse erfolgreich beendet werden kann.

Es werden typischerweise eine Reihe sehr verschiedener Datenarten ausgewertet. Festplatten werden analysiert, um Schadprogramme zu finden und zu untersuchen, was die Täter auf den Systemen getan haben. Firewall- und Proxy-Logdaten werden auf Rückmeldekanäle und Datenabflüsse ausgewertet. Die Logdaten des Verzeichnisdienstes geben Hinweise auf untypische Logins, die auf kompromittierte Zugangsdaten hindeuten. Netzwerkmitschnitte werden untersucht, um verschlüsselten Verkehr der Täter zu entziffern. Speziell auf den Vorfall angepasste Detektionstools werden auf allen Systemen im Netzwerk ausgerollt und deren Logdaten werden ausgewertet. Nicht zuletzt werden Schadprogramme analysiert, um Indikatoren zur Detektion zu erarbeiten.

Es ist offensichtlich, dass diese Analysefähigkeiten nur von einem Team von Experten abgedeckt werden können. Auch das BSI hält kein vordefiniertes Team vor, das auf Abruf ausrücken kann, sondern zieht bei Bedarf Experten aus mehreren Bereichen zusammen. Einzelne Analysebereiche können aus Ressourcengründen von Dienstleistern durchgeführt werden.

Externe Einflüsse

Die Analysen gehen nicht isoliert vom Rest der Welt vonstatten. Es entstehen berechtigte Fragen seitens der Nutzer, deren Rechner kopiert und untersucht werden müssen. Sie treibt die Sorge um, ob sie sicher an vertraulichen Dokumenten arbeiten können, oder ob sie davon ausgehen müssen, dass Täter Zugang zu Mails und Dateiablagen hatten oder haben. Solche Analysen haben stets eine technische und eine öffentlichkeitswirksame Komponente, die gegeneinander abgewogen werden wollen. Erschwert wird dies, wenn



Die Auswertungen von Firewall- und Proxy-Logdaten geben Aufschlüsse über die Aktivitäten der Angreifer.

Mitarbeiter aufgrund der spärlich verfügbaren Informationen anfangen zu spekulieren und nicht zutreffende Aussagen über den Zustand des Netzwerks getroffen werden.

Das Ergebnis

Nicht in allen Fällen wird der sogenannte Patient Zero, also das zuerst infizierte System, erkannt. Das liegt daran, dass der Angriff oftmals schon lange zurückliegt, bevor die Untersuchung beginnt. Daher stehen nicht mehr alle benötigten Logdaten zur Verfügung.

Bekannt ist aber, dass professionelle Täter prinzipiell alle Angriffsarten nutzen, die in der IT-Sicherheit existieren. Am häufigsten sind präparierte E-Mails, die auf den speziellen Empfänger zugeschnitten sind und einen Link auf Schadcode oder einen Anhang mit Malware enthalten. Verbreitet sind aber auch sogenannte Watering-Hole-Angriffe, bei denen Webseiten, die für das Zielpublikum relevant sind, angegriffen und mit bösartigem Code versehen werden. Besuchen die Zielpersonen die Webseite, wird durch den Schadcode eine Hintertür auf ihrem Rechner installiert. Nach wie vor gibt es auch noch das klassische Hacking, indem Webserver oder andere Systeme, die von außen über das Internet erreichbar sind, angegriffen werden. Gemeinsam ist all diesen Angriffsarten, dass die Täter es nicht bei dem initial kompromittierten Rechner belassen, sondern ihn als Eintrittspunkt nutzen, um sich weiter im internen Netzwerk auszubreiten. Dafür laden sie weitere Schadprogramme und Werkzeuge nach und spähen im Arbeitsspeicher hinterlegte Zugangsdaten aus.

Das Ziel der Täter ist stets, sich langfristigen Zugang zum Netzwerk zu sichern. Besonders wertvoll sind Zugangsdaten mit hohen Systemrech-

ten. Mit diesen Zugangsdaten können sich die Täter beliebig im Netzwerk ausbreiten und auf sensitive Systeme zugreifen. In vielen Fällen ist eine ihrer ersten Ziele der Domain Controller, der in einem Netzwerk alle Zugangsdaten und Berechtigungen verwaltet. Wenn die Täter diesen kompromittieren, ist das Netzwerk grundlegend kompromittiert und kann nicht mehr durch den Austausch einzelner Rechner bereinigt werden. Durch die Übernahme dieser zentralen Systeme erhalten Täter Zugriff auf sämtliche Zugangsdaten, inkl. solcher für VPN-Einwahl.

Die Bereinigung

Eine der umstrittensten Fragen bei jedem Vorfall ist die, ob man bereits bekannte infizierte Systeme sofort bereinigen und erkannte Rückmeldekanäle umgehend sperren soll. So intuitiv diese Vorgehensweise zunächst klingt, ist sie meistens kontraproduktiv. Durch diese Maßnahmen erfahren Täter, dass sie entdeckt wurden und ihre Aktivitäten untersucht werden. Dies führt dazu, dass sie Spuren verschleiern und ihre Vorgehensweise ändern. Die Analysten haben in der frühen Phase der Untersuchung noch keinen Gesamtüberblick darüber, welche Schadprogramme und Tools die Täter benutzen, welche Zugangsdaten sie verwenden und auf welchen Systemen sie Hintertüren besitzen. Das gesamte Netzwerk kann also noch nicht bereinigt werden, die Täter werden immer noch Zugang haben, selbst wenn einige Rechner bereinigt werden. Zudem sind die Täter in den meisten Fällen bereits Monate im Netzwerk aktiv und haben möglicherweise schon einen Großteil der für sie interessanten Daten gestohlen. Aus diesen Gründen empfiehlt das BSI, zunächst die dafür notwendige Zeit zu investieren, den Vorfall vollständig zu untersuchen. Dies kann durchaus mehrere Wochen oder Monate dauern. Erst wenn ein zusammenhängendes Bild von dem Vorfall vorliegt, kann ein Plan entwickelt werden, wie das Netzwerk vollständig bereinigt und gegen zukünftige Angriffe abgehärtet werden kann. Wenn beispielsweise das Active Directory kompromittiert wurde, führt kein Weg an einem organisationsweiten Passwort-Reset und einem Neuaufbau des Active Directory vorbei.

Um zukünftige Angriffe dieser Art abwehren zu können, empfiehlt sich beispielsweise ein Konzept namens „ESAE — Enhanced Secure Administrator Environment“. Dieses härtet das Active Directory und Administratoren-Arbeitsplätze und isoliert sie weitgehend vom restlichen Netzwerk. Die Prämisse dabei ist, dass ein einzelner infizierter Arbeitsplatz-PC nicht mehr dazu führen darf, dass die gesamte Windows-Domäne kompromittiert wird. Um die Ausbreitung im Netz zu verhindern, werden über Personal Firewalls und Gruppenrichtlinien im Domain Controller Verbindungen zwischen Arbeitsplatz-PCs unterbunden.

Um in Zukunft Angriffe schneller entdecken zu können, empfiehlt es sich, ein Security-Monitoring-Konzept umzusetzen, das die kontinuierliche Auswertung von Log- und Sensordaten vorsieht. Zudem sollten die Nutzer sensibilisiert werden, um Angriffe über Social Engineering besser erkennen zu können.

Fazit

Die Aspekte, welche die Vorfallsbearbeitung positiv beeinflussen, sind zum einen, dass die betroffene Institution den Vorfall als ernst akzeptiert und nicht als Teil des Tagesgeschäfts des IT-Betriebs marginalisiert. Weiterhin sollte nicht nach Schuldigen gesucht , sondern konstruktiv daran gearbeitet werden, zukünftige Angriffe zu verhindern. Entscheidend ist, dass für die Untersuchung genügend Zeit eingeräumt und nicht darauf gedrungen wird, auf einer unzureichenden Erkenntnislage die Bereinigung durchzuführen, die so eventuell nicht das volle Ausmaß der Kompromittierung erkennt . Ein Vorfall ist nicht mit Bereinigung von Schadcode-beziehungsweise mit der Neuinstallation abgeschlossen. Die vom Analyseteam identifizierten Mängel müssen behoben und die vorgeschlagenen Sicherheitsmaßnahmen umgesetzt werden, um zukünftige Attacken zu verhindern oder zumindest zu erschweren. ●

Timo Steffens,
Referat Lagezentrum und CERT-Bund

Anzahl der erfolgreichen Cyber-Angriffe nimmt zu

Das sagen die Zahlen der Cyber-Sicherheitsumfrage 2015. Bereits zum zweiten Mal führte das BSI mit Unterstützung des Bundesverbandes der Deutschen Industrie (BDI), des Bundesverbandes Informationswirtschaft, Telekommunikation und neue Medien (Bitkom), des Deutschen Industrie- und Handelskammertages (DIHK), der Gesellschaft für Informatik e.V. (GI), des Verbandes der IT-Anwender (VOICE), des Verbandes der Maschinen- und Anlagenbauer (VDMA) und des Zentralverbandes Elektrotechnik- und Elektronikindustrie (ZVEI), die Cyber-Sicherheitsumfrage durch. Die Fortschreibung der Zahlen aus dem Vorjahr zeigt, dass die Cyber-Sicherheitslage für Unternehmen und Behörden weiter angespannt bleibt.
Die Befragung wurde als Online-Umfrage mit 18 geschlossenen Fragen im Zeitraum von Juni bis September 2015 realisiert. Insgesamt wurden 424 Unternehmensdatensätze ausgewertet.

1

Ziel von Angriffen

58,5 % der befragten Institutionen und Unternehmen haben ***festgestellt***, dass sie ***Ziel von Cyber-Angriffen*** waren. Dies umfasst erfolgreiche als auch abgewehrte Angriffe.

30,3 % der befragten Institutionen haben keine Angriffe festgestellt.

11,3 % gaben keine Antwort.

Von den festgestellten Angriffen konnten ...

42,7 % *nicht abgewehrt* werden. Die Angreifer waren in diesen Fällen erfolgreich.

42,3 % konnten die festgestellten Angriffe abwehren.

11,3 % der Fälle wurden Auswirkungen registriert, die jedoch nicht zweifelsfrei auf Cyber-Angriffe zurückgeführt werden konnten.

3,6 % gaben keine Antwort.

2

Art der festgestellten Angriffe

72,2 % waren beliebige und **ungezielte Infektionen mit Malware** mittels Drive-by-Download über Webseiten-Banner oder via E-Mail-Spam.

30,6 % waren **(D)DoS-Angriffe** auf die Internetauftritte der Institutionen.

21 % waren **gezielte Infektionen** mit Malware via Social-Engineering per E-Mail oder über einen USB-Stick.

19,8 % Angriffe mit dem Ziel der **Übernahme der IT-Systeme** zum anschließenden Missbrauch für Angriffe auf weitere Systeme.

3

Primäre Einfallstore

31,8 %
Fehlkonfigurationen von Systemen.

35,9 %
nicht eingespielte Patches.

54,1 %
unbeabsichtigtes Fehlverhalten von Mitarbeitern.

43,2 %
bisher unbekannte Schwachstellen ohne verfügbare Patches (sogenannte 0-Day-Lücken).

4 Die wirtschaftlichen Schäden durch Angriffe sind kaum zu beziffern

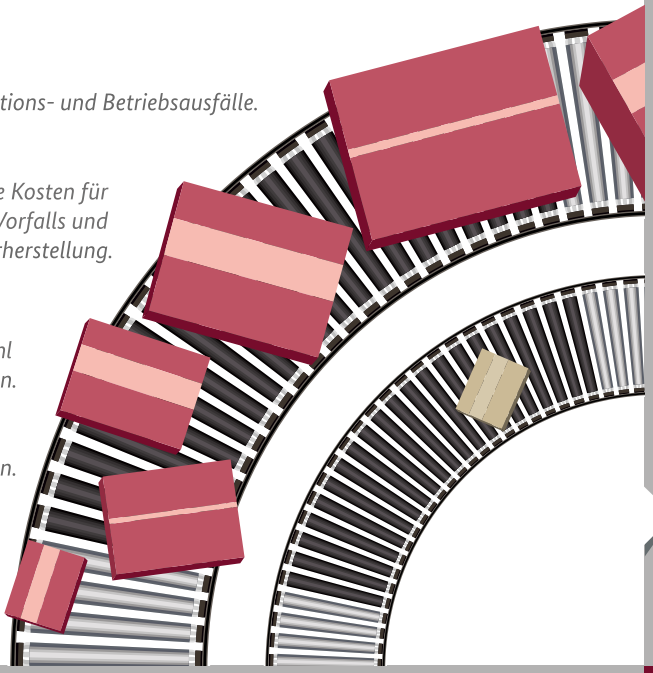
19,1 % Produktions- und Betriebsausfälle.

15,1 % erhebliche Kosten für die Aufklärung des Vorfalls und die Systemwiederherstellung.

8,5 % Diebstahl digitaler Identitäten.

8,3 % Reputationsschaden.

5,7 % Diebstahl wirtschaftlich bedeutender Daten.



5 Betrieb einstellen

46,2% der befragten Institutionen müssten nach Cyber-Angriffen vorübergehend ihren Betrieb einstellen.

6 Der Druck steigt

Für **70,2%** der Institutionen haben die Risiken durch Cyber-Angriffe zugenommen.

7 Die bedrohlichsten Cyber-Angriffe der nächsten Jahre

63% der befragten Institutionen erwarten **primär gezielte Infektionen mit Malware** via Drive-by-Download oder E-Mail-Spam,

59,2% **Datendiebstahl** durch Eindringen in Systeme,

47,4% APT: **Eindringen in Systeme** zur langfristigen Infiltration und

46,7% **ungezielte Infektion** mit Malware.

8 Nachholbedarf beim Schutz gegen Cyber-Angriffe: Umgesetzte Maßnahmen

Ja	Nein	
20,8 %	79,2 %	Einsatz sicherer Browser oder sicherer Surfumgebungen.
31,4 %	68,6 %	strukturiertes Informationssicherheits-Management (ISMS).
51,7 %	48,3 %	regelmäßige Maßnahmen zur Sensibilisierung aller Mitarbeiter.
52,8 %	47,2 %	Verschlüsseln der Datenträger.
64,4 %	35,6 %	strukturiertes oder zentralisiertes Patchmanagement.
84,4 %	15,6 %	dezentrale Abwehr von Schadprogrammen durch AV-Software auf Client-/Server-Systemen.
85,6 %	14,4 %	zentrale Abwehr von Schadprogrammen über Sicherheitsgateway bzw. Mailserver.
95,5 %	4,5 %	Sichern der Netzübergänge (Sicherheitsgateways, Firewalls, IDS/IPS, usw.).

9 Planung

59% der befragten Institutionen planen mittelfristig weitere Verbesserungen ihrer IT-Sicherheit.

15,3% müssen kurzfristig in kritischen Bereichen nachbessern.

Die vollständigen Ergebnisse der Cyber-Sicherheitsumfrage 2015 sind unter folgender Adresse zu finden: www.cybersicherheitsumfrage.de

„Es gibt viel zu tun”

Interview mit Klaus Vitt, seit Oktober 2015 Staatssekretär im Bundesministerium des Innern und Beauftragter der Bundesregierung für Informationstechnik

Herr Staatssekretär, zu Ihrem Aufgabenbereich gehört die Abteilung „Informationstechnik, Digitale Gesellschaft und Cyber-Sicherheit”. Das ist ein weites Feld. Wo wollen Sie dort besondere Akzente setzen?

Ich habe mir vier Schwerpunkte gesetzt, die ich als Bundesbeauftragter für Informationstechnik voranbringen möchte: die Digitalisierung des Asylverfahrens, die Konsolidierung der IT in der Bundesverwaltung, die Konsolidierung der IT-Netze des Bundes und die IT- und Cyber-Sicherheit.

Welche Rolle wird dabei der letztgenannte Punkt spielen?

Die Sicherheit der Informationstechnik ist Grundlage jeder Form von Digitalisierung. Fragen der IT- und Cyber-Sicherheit spielen daher in meinem Aufgabenbereich eine zentrale Rolle. Das Ende Juli 2015 in Kraft getretene IT-Sicherheitsgesetz sehe ich als einen ersten wichtigen Schritt, damit die IT-Systeme und digitalen Infrastrukturen Deutschlands künftig zu den sichersten weltweit gehören.

Wie würden Sie die Rolle des BSI in diesem Zusammenhang beschreiben?

Mit dem BSI haben wir in Deutschland seit vielen Jahren ein staatliches Kompetenzzentrum für Fragen der IT- und Cyber-Sicherheit, dessen fachliche Expertise weit über den Bereich der öffentlichen Verwaltung hinaus anerkannt ist. Es hat einen klaren gesetzlichen Auftrag, den wir zuletzt durch das IT-Sicherheitsgesetz noch einmal deutlich erweitert haben. Damit ist das BSI in Fragen der IT-Sicherheit zum zentralen Akteur für die Betreiber Kritischer Infrastrukturen geworden. Hier geht es um Mindeststandards an IT-Sicherheit, Meldepflichten bei erheblichen IT-Sicherheitsvorfällen, aber auch um einen aktiven Part des BSI: Bei gemeldeten erheblichen IT-Sicherheitsvorfällen sind die anderen Betreiber vom BSI schnellstmöglich zu informieren.

> **Das IT-Sicherheitsgesetz ist ein erster wichtiger Schritt, damit die IT-Systeme und digitalen Infrastrukturen Deutschlands künftig zu den sichersten weltweit gehören.**

Andere europäische Staaten haben keine so eindeutige Trennung zwischen IT-Sicherheitsbehörde und Nachrichtendienst wie Deutschland. Ist dieser Sonderweg trotz der Bedrohungslage noch der richtige?

Die Gründung des BSI im Jahr 1991 war eine sehr kluge und vorausschauende Entscheidung. Durch die Trennung der „Code breaker“ von den „Code makern“ konnte das BSI über die Jahre hinweg in der Öffentlichkeit und insbesondere in der Wirtschaft großes Vertrauen aufbauen. Für eine gedeihliche Zusammenarbeit zwischen Staat und Wirtschaft ist dies unerlässlich.

Es kann wohl keine hundertprozentige IT-Sicherheit geben. Aber können wir gleichwohl noch Optimierungspotenziale erschließen?

Cyber-Sicherheit entsteht in einer sicheren Umgebung. Der Cyber-Raum ist nur so sicher, wie es die dort angeschlossenen Systeme und Infrastrukturen sind. Weder Staat noch Wirtschaft können die IT- Sicherheit in unserem Land alleine erreichen: Jeder muss seinen Teil dazu beitragen. Die Kooperation zwischen Staat und Wirtschaft wird bei der Gewährleistung von IT-Sicherheit künftig eine zentrale Rolle spielen.

Sie haben langjährige Erfahrung in der Wirtschaft gesammelt, bei Software- und Computerherstellern ebenso wie in der Telekommunikation: Ist die deutsche Wirtschaft ganz generell sensibel und gerüstet genug für die Herausforderungen der IT-Sicherheit?

Dort wo sich Wertschöpfungsstrukturen fundamental verändern, steht IT-Sicherheit regelmäßig nicht an erster Stelle. Mein Eindruck ist jedoch, dass sie mehr und mehr als notwendige Infrastruktur verstanden wird. Keine verlässliche Produktion, kein eCommerce ohne IT-Sicherheit. Kompliziert wird es dann jedoch bei der Umsetzung: Wie sieht meine Gefährdungssituation aus und wie schütze ich mich in einer

Kurzprofil Klaus Vitt
Klaus Vitt (geb. 1952) studierte Nachrichtentechnik an der Fachhochschule der Deutschen Bundespost und Mathematik/Informatik an der Universität in Dortmund. Nach ersten Berufserfahrungen in verschiedenen IT-Unternehmen sowie der Bertelsmann AG war er zehn Jahre in verantwortlichen Positionen im IT-Bereich bei der Deutschen Telekom AG tätig. Von 2006 bis 2015 arbeitete er in der Bundesagentur für Arbeit, zunächst als Geschäftsführer der zentralen IT und anschließend als Generalbevollmächtigter für IT und Prozessmanagement. Seit Oktober 2015 ist Klaus Vitt Staatssekretär im Bundesministerium des Innern und Beauftragter der Bundesregierung für Informationstechnik.

wirtschaftlich vertretbaren Art und Weise? Brauche ich Unterstützung und wer bietet eigentlich vertrauenswürdige und sichere Produkte und Dienstleistungen an?

Wo und wie kann hier nachgebessert werden?
Verfügbarkeit, Vertraulichkeit und Integrität der Daten und Informationen werden wir künftig nur gewährleisten können, wenn Staat und Wirtschaft noch enger als bisher zusammenarbeiten. Hierzu müssen wir gegebenenfalls auch neue Formen der Zusammenarbeit entwickeln. Mit der Deutschen Cyber-Sicherheitsorganisation (DCSO) haben wir mit der Wirtschaft einen neuen Weg eingeschlagen.

Sie haben das IT-Sicherheitsgesetz angesprochen; derzeit werden in zwei Körben die entsprechenden Verordnungen erarbeitet. Welche Erfahrungen machen Sie im Hinblick auf die Kooperationsbereitschaft?
Wir verfolgen mit dem IT-Sicherheitsgesetz ja bewusst einen kooperativen Ansatz. Es geht um ein vertrauensvolles Miteinander von Staat und Wirtschaft. Das erleben wir bereits bei der Vorbereitung der Verordnung im UP KRITIS. Zunächst werden wir vier der sieben mit dem Gesetz adressierten Sektoren, nämlich Energie, Wasser, Ernährung sowie Informations- und Kommunikationstechnik, in der Verordnung abbilden. Bis Ende 2016 folgen dann die übrigen Sektoren Transport und Verkehr, Gesundheit, Finanz- und Versicherungswesen. Dass dies so zügig möglich ist, basiert maßgeblich auch auf der kooperativen und engagierten Zusammenarbeit mit den adressierten Wirtschaftsbranchen im UP KRITIS.

Sie haben eingangs auch den Schutz der Netzinfrastruktur des Bundes erwähnt. Setzen Sie auch dort auf die Zusammenarbeit mit der deutschen Wirtschaft?
Um die Kommunikation von Regierung und Bundesverwaltung auch zukünftig erfolgreich zu schützen, verfolgen wir mit dem Projekt „Netze des Bundes“ ein umfangreiches Konsolidierungsprogramm. Bei der Auswahl leistungsfähiger Dienstleister für das Projekt spielt die Vertrauenswürdigkeit eine große Rolle. Es ist für uns entscheidend, dass der Partner willens und tatsächlich in der Lage ist, vertrauliche Informationen vertraulich zu behandeln. Auch sollten die Datenströme zwischen den Bundesbehörden stets in Deutschland verbleiben. Hier haben wir in der Vergangenheit positive Erfahrungen mit der deutschen Wirtschaft gemacht und werden daher auch in Zukunft auf eine Zusammenarbeit mit nationalen Partnern setzen.

Sie sind „vom Fach“, haben Nachrichtentechnik, Mathematik und Informatik studiert. War der gewaltige Bedeutungszuwachs der IT-Sicherheit damals schon absehbar?
In diesem Ausmaß sicherlich nicht! Die zunehmende digitale Verwundbarkeit in allen Bereichen unseres Lebens und Handelns wird in den kommenden Jahren zu einer der zentralen Herausforderungen für unsere Gesellschaft. Für uns alle bedeutet das: Es gibt viel zu tun! ●

Der Beauftragte der Bundesregierung für Informationstechnik:
www.cio.bund.de

Cloud Computing

Game Changer für die Informationssicherheit

Cloud Computing mag als Hype vor gut fünf Jahren begonnen haben. Mittlerweile stehen für Unternehmen zwar noch viele Fragen zur Sicherheit im Raum, damit die produktive Arbeit in der Cloud tatsächlich beginnen kann. Doch alle Zeichen deuten darauf hin, dass sich aus dem Hype eine Technologie entwickelt hat, die bleiben wird. „The cloud is here to stay“ - denn sie bietet Unternehmen, ob als Nutzer oder Anbieter, in Zukunft Vorteile, wenn diese jetzt klare Vorkehrungen für ihre Sicherheit treffen. Nur wer die Konsequenzen für die IT-Sicherheit, die sich aus dem Cloud Computing ergeben, kennt, ist handlungsfähig.

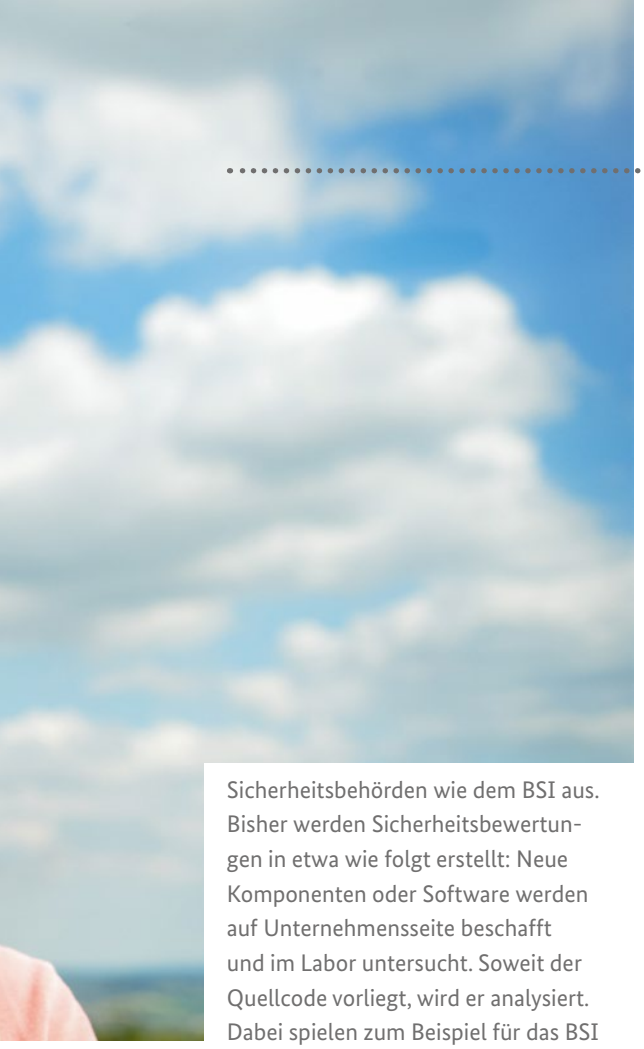
Befeuert durch den Effizienzgewinn aus der Virtualisierung winken Cloud-Nutzern Kostenersparnisse für ihre IT. Dank der mittlerweile weit verfügbaren Breitband-Anbindungen können IT-Ressourcen, -Plattformen und -Anwendungen heute von zahlreichen Unternehmen angeboten und genutzt werden. Hierbei stellt sich für viele IT-Verantwortlichen die Frage „Kaufen oder Mieten?“ neu. Denn wer lediglich einmal im Jahr einen Bericht zu erstellen hat, muss heute kein Programm für mehrere Tausend Euro dafür kaufen, wenn der erforderliche Service manchmal für weniger als fünfzig Euro pro Monat gemietet werden kann. Und auch die Cloud-Hersteller haben Vorteile. Umsatzschwankungen für neue Versionen von Anwendungen und Programmen fallen geringer aus, weil eine relativ konstante Nutzerschaft monatliche Einnahmen generiert, die besser planbar sind.

Skeptiker sehen im Cloud Computing Potenziale für einen Personalabbau, wenn der IT-Betrieb an Cloud-Anbieter ausgelagert wird. Doch wird es für Unternehmen gefährlich, wenn sie dem Irrglauben unterliegen, die Verantwortung für die Sicherheit ihrer IT einfach mit abgeben zu können.

Sicher ist, dass sich für viele Instanzen wie Sicherheitsbehörden und Unternehmen die Vorgehensweisen in Sachen IT-Sicherheit drastisch ändern. Dies erfordert neue Prozesse und Kompetenzen.

Game Changer 1: Einfluss auf die Arbeit von Sicherheitsinstitutionen

Cloud Computing ist nicht nur eine neue Technik, wie etwa das Tablet gegenüber dem Laptop, sondern es zieht große Umwälzungen für die Informationssicherheit nach sich und ist damit ein wahrer „Game Changer“. Dies wirkt sich auch auf das Tätigkeitsfeld von



Sicherheitsbehörden wie dem BSI aus. Bisher werden Sicherheitsbewertungen in etwa wie folgt erstellt: Neue Komponenten oder Software werden auf Unternehmensseite beschafft und im Labor untersucht. Soweit der Quellcode vorliegt, wird er analysiert. Dabei spielen zum Beispiel für das BSI als Fachbehörde Fragen wie „Leitet der Router die Datenpakete so weiter, wie er es soll?“ und „Ist die Plattform beim Surfen im Internet anfällig und wenn ja, wodurch?“ eine Rolle für die Bewertung des eingesetzten Produkts. Eine solche Bearbeitung funktioniert allerdings nur dann, wenn Komponenten in ein Labor gebracht werden. Bei Anwendungen, die als Dienst im Internet angeboten werden, ist eine Untersuchung auf diese Weise nicht mehr möglich. Und die Cloud-Anbieter sind – wenn sie nicht gerade in einem Zertifizierungsverfahren stecken – meist sparsam beim Einräumen von Prüfmöglichkeiten. Außerhalb von Zertifizierungsverfahren ist die Überprüfung der Sicherheit von IT-Diensten mit den altbewährten Methoden daher nicht mehr möglich.

Game Changer 2: Änderung von Unternehmensstrategien

Der wesentliche positive ökonomische Aspekt des Cloud Computings liegt in der Masse. Denn hohe Nutzerzahlen ermöglichen Skaleneffekte, welche die Wettbewerbsfähigkeit und den Gewinn seitens des Anbieters steigern. Die Wahlmöglichkeit des Nutzers für oder gegen die Cloud wird künftig kaum oder gar nicht mehr bestehen. Zahlreiche große Anbieter wie Microsoft oder Adobe bieten ihre Produkte und Services jetzt schon vorrangig als Abonnement-Modell über die Cloud an. Microsoft etwa verfolgt explizit die Strategie, in Zukunft nur noch Anwendungen für seine Microsoft Azure Cloud zu entwickeln. Das bedeutet für den Nutzer: Wer heute Windows oder Microsoft Office verwendet, bezieht künftig seine IT-Werkzeuge aus der Azure Cloud. Wer dabei Sicherheitsbedenken hat, muss gründlich abwägen, ob diese so schwerwiegend sind, dass eine komplette Migration beispielsweise zu Linux und LibreOffice vertretbar wäre.

Game Changer 3: Einflüsse auf die Zertifizierung

Bei der Zertifizierung von Informationssicherheits-Managementsystemen (beispielsweise nach ISO 27001) herrscht die implizite Annahme, dass der Auditor erst das Live-System zu sehen bekommt. Kurzfristige Änderungen daran sind zu aufwendig. Kommen hingegen Cloud-Dienste zum Einsatz, trifft diese These nicht mehr zu. Denn ein virtualisiertes Rechenzentrum kann in kürzester Zeit umgezogen und ebenso schnell vollständig umkonfiguriert werden. Ein komplexes Zonensystem mit vielen Paketfiltern, sogenannten demilitarisierten Zonen (DMZ), hat Sicherheitsvorteile, kostet jedoch Ressourcen, die dem Anbieter nicht für weitere Kunden zur Verfügung stehen. Nutzt der Cloud-Anbieter die Möglichkeiten der Elastizität und Flexibilisierung, um kurzfristig die Cloud-Infrastruktur umzukonfigurieren, so kann er Ressourcen von Sicherheitsdiensten für neue Kunden verwenden. Dies können heutige Zertifizierungsverfahren nicht ausschließen. In virtuellen Infrastrukturen müssen keine Techniker ausrücken, um Kabel neu zu ziehen oder Server neu zu starten. Ein Administrator kann all das nun per Knopfdruck ausführen. Damit stellt sich die Frage, wie valide und aussagekräftig in Zukunft Zertifikate noch sind.

Fatalismus ist keine Option: Ein Ansatz für sicheres Cloud Computing

Wie sich zeigt, ist Cloud Computing also ein Game Changer, der eine neue Definition von IT-Sicherheit in vielen Bereichen erfordert. Fatalistisch auf diese Veränderungen zu reagieren und den Kopf in den Sand zu stecken, wäre die falsche Reaktion. Sicheres Cloud Computing benötigt ein großes Maß an Vertrauen, und Vertrauen kann nur durch Transparenz entstehen. Diese gliedert sich in drei Bereiche:

Informationen des BSI zu sicherem Cloud Computing

Die Webseite des BSI zum sicheren Cloud Computing unter www.bsi.bund.de/cloud liefert Ihnen zielgruppengerecht umfassende Materialien – für CEOs und CIOs sowie für Mitarbeiter auf operativer Ebene. Des Weiteren stehen umfassende Tipps zur Risikoanalyse aus Kundensicht auf der Seite zur Verfügung.

Fatalismus ist keine Option: Ein Ansatz für sicheres Cloud Computing

1 Risikotransparenz

2 Offene Standards

3 Klare Aufteilung der Verantwortung zwischen Nutzer und Anbieter

Transparenz bei Risiken (und Chancen) des Cloud Computings

Das BSI trägt zur Risikotransparenz beim Cloud Computing bei, indem es bestehende Risiken systematisch erfasst und bewertet. Ziel ist es, alle Akteure aus Politik, Wirtschaft und Gesellschaft in die Lage zu versetzen, gut begründete Entscheidungen zur Nutzung oder auch zur Nichtnutzung von Cloud-Diensten zu treffen. Hierbei ist es notwendig, zwischen sicheren Clouds und sicherem Cloud Computing zu unterscheiden.

Das Ideal einer sicheren Cloud ist unerreichbar, denn absolute Sicherheit ist nicht existent. Entscheidend ist es, Prozesse so sicher wie möglich zu gestalten, indem sie genau analysiert werden. Nicht sichere Clouds stehen im Fokus, sondern eben sicheres Cloud Computing. Dazu müssen Sicherheitsanforderungen erstellt und im Zuge des Cloud Computings umgesetzt werden. Dies ist ein iterativer und dynamischer Prozess.

Ob ein Cloud-Dienstleister die Anforderungen des Kunden erfüllt, ist eine Frage des Risikomanagements, das auf Kundenseite individuell erfolgen muss. Zwei verschiedene Kunden eines Anbieters werden bei dieser Frage höchstwahrscheinlich zu zwei unterschiedlichen Bewertungen kommen. Risikotransparenz bedeutet, dass sie begründete Entscheidungen treffen können. Risikotransparenz ist also ebenso nötig wie Chancentransparenz.

Offene Standards schaffen Vertrauen für das Cloud Computing

Der Einsatz offener Standards für die Sicherheit und eine Offenlegung darüber, wie die Sicherheit von IT-Systemen überprüft wird, gehören zu den Grundforderungen des BSI. Sie gelten auch für die Cloud. Nur so kann das Risikomanagement bewerten, welches Sicherheitsniveau die Geschäftsprozesse in der Cloud haben müssen, und folglich entscheiden, ob Cloud Computing eine Option darstellt oder nicht. Das BSI arbeitet daher fortlaufend auch in Kooperation mit europäischen Partnern wie dem ANSSI in Frankreich an offenen Standards für sicheres Cloud Computing. Der Anforderungskatalog Cloud Computing kann im Rahmen von ISAE 3000 mit SOC-2-Berichten durch Wirtschaftsprüfer testiert werden. Dabei wird nicht nur geprüft, ob eine Anforderung zu einem bestimmten Zeitpunkt bestand, sondern insbesondere auch, ob die damit verbundenen Maßnahmen über einen gewissen Zeitraum umgesetzt wurden.

Sicherheitsverantwortung kann nicht in die Cloud migriert werden

Verantwortung kann nicht ausgelagert werden und staatliche Garantien zur Sicherheit von Cloud-Diensten, etwa in Form einer Lizenzierung, stehen in naher Zukunft nicht in Aussicht. Daher ist eine klare Aufteilung der Verantwortlichkeiten zwischen Nutzer und Anbieter nötig, bevor Cloud-Services in Anspruch genommen werden.

Der Nutzer sollte alle für ihn relevanten Aspekte der IT-Sicherheit klar vertraglich vereinbaren, und zwar sowohl präventive wie auch reaktive Maßnahmen. Dazu erfordert es Antworten auf die Fragen: Was passiert bei einem Sicherheitsvorfall? Wie ist die Informationskette bei einem Ausfall geregelt? Ist eine Einflussnahme darauf möglich, wie der Anbieter die Vorfälle behandelt? Welche Folgen ergeben sich aus möglichen Verletzungen der Vereinbarungen?

Die jeweiligen Verantwortlichkeiten müssen im Vorfeld genau geregelt werden, sonst wird aus unorganisierter Verantwortlichkeit organisierte Verantwortungslosigkeit. ●

Dr. Patrick Grete, Referat Mindeststandards und Produktsicherheit

Sicherheit lebt vom Dialog: Fragen Sie das BSI

Risikobewertungen, Sicherheitsmaßnahmen und Sicherheitsstandards können nur im Dialog mit Cloud-Anbietern und Nutzern weiterentwickelt werden. Fragen, Anmerkungen und konkrete Empfehlungen nehmen wir über cloudsecurity@bsi.bund.de gerne jederzeit entgegen. Fragen zum Thema Zertifizierung können Sie jederzeit an zertifizierung@bsi.bund.de richten.

Höchstmaß an Fälschungssicherheit

Zehn Jahre elektronische Ausweisdokumente

Seit gut einem Jahrzehnt erhöhen elektronische Komponenten die Fälschungssicherheit hoheitlicher Ausweisdokumente, beschleunigen Grenzkontrollen an Flughäfen und machen den digitalen Identitätsnachweis im Internet möglich. Nachdem der Reisepass bereits 2005 einen integrierten elektronischen Chip erhielt, folgten später auch der Personalausweis und der Elektronische Aufenthaltstitel, sodass mittlerweile alle Ausweisdokumente auf dem gleichen technischen Familienkonzept basieren. Jüngstes Familienmitglied ist ein neues Dokument: der Ankunftsnachweis für Asylsuchende.

Reisepass

Die Einführung des Reisepasses mit Chip in Deutschland erfolgte in zwei Stufen. Seit dem 1. November 2005 werden auf dem Chip das biometrische Lichtbild und seit 1. November 2007 zusätzlich zwei Fingerabdrücke gespeichert. Heute, zehn Jahre nach der Einführung, enthalten alle gültigen deutschen zentral produzierten Reisepässe einen solchen Chip.
Der ePass ermöglicht es, in den Grenzkontrollen automatisierte Prozesse auf hohem Sicherheitsniveau zur Effizienzsteigerung zu etablieren. So kann heute an den passagierstärksten deutschen Flughäfen das Grenzkontrollsystem EasyPASS von jedem Reisenden mit einem europäischen Reisepass oder dem elektronischen Personalausweis genutzt werden. EasyPASS prüft innerhalb von Sekunden die Echtheit des Dokuments und führt einen biometrischen Vergleich des Gesichts des Reisenden mit dem im Pass gespeicherten Passbild durch. Der Einsatz ähnlicher Systeme nimmt weltweit zu.

Aber auch die Qualität der klassischen Ausweiskontrolle profitiert von den elektronischen Daten, da die Echtheit von Pässen kryptografisch verifiziert werden kann und dem Grenzbeamten ein höherwertiges Gesichtsbild aus dem Chip zur Verfügung steht.

Personalausweis

Mit der Einführung der neuen Generation des Personalausweises zum 1. November 2010 und dem elektronischen Aufenthaltstitel (eAT) knapp ein Jahr später, am 1. September 2011, wurde die Strategie des sicheren und elektronischen Identitätsnachweises

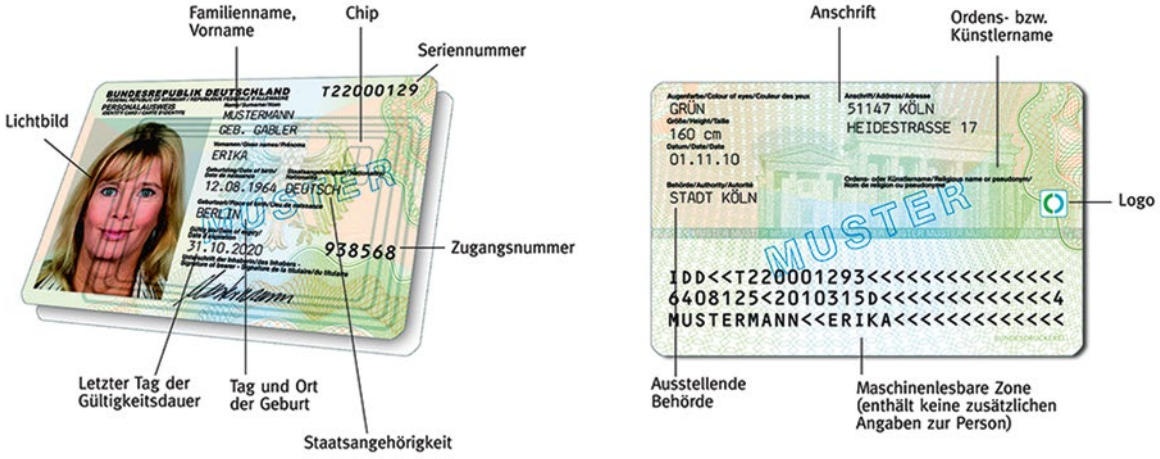
konsequent fortgeführt. Denn zusätzlich zur Biometriefunktion bieten die neuen Dokumente die Möglichkeit zur sicheren Identifizierung im Internet (Elektronischer Identitätsnachweis), etwa für eGovernment-Anwendungen, im Rahmen derer Bürgerinnen und Bürger Verwaltungsprozesse einfach online abwickeln können. Schließlich kann mit dem Ausweis auch eine elektronische Unterschrift geleistet werden (qualifizierte Signatur).
Fünf Jahre nach der Einführung sind rund 40 Millionen Personalausweise und Aufenthaltstitel der neuen Generation ausgestellt, sodass ein Großteil der Bürgerinnen und Bürger mit diesem

1 .Januar 2015 angemeldeten Fahrzeuge einfach im Internet mit dem Personalausweis abgemeldet werden.
Daneben werden im Rahmen der eID-Strategie von Bund und Ländern Servicekonten für Bürgerinnen und Bürger eingerichtet, bei denen eine Anmeldung mit dem elektronischen Identitätsnachweis möglich ist und die möglichst viele Verwaltungsdienstleistungen via Web abdecken.
Weitere Gesetzesinitiativen wurden gestartet oder sind bereits abgeschlossen. Nach dem eGovernment-Gesetz (E-GovG) sind Behörden des Bundes verpflichtet, in Verwaltungsverfahren, „in denen diese die Identität einer

Alternative kann auch ein zusätzlicher Bluetooth-Leser dienen. Es ist zu erwarten, dass die mobile Anwendung in Zukunft immer stärkere Bedeutung gewinnen wird.

Technisches Familienkonzept: eine Technik für alle Dokumente

Das technische Rückgrat für alle elektronischen ID-Dokumente stellen mehrere technische Spezifikationen und Schutzprofile des BSI – ein modulares, technisches Familienkonzept. Das bedeutet, dass sowohl ePass, Personalausweis und Aufenthaltstitel Dokumentenprofile dieser Spezifikationen sind



Der neue Personalausweis wird seit 1. November 2010 im Scheckkartenformat ausgestellt und enthält zahlreiche Sicherheitsmerkmale, die eine Fälschungssicherheit auf höchstem Niveau gewährleisten.

Dokument ausgestattet ist und es sich deshalb für Dienstanbieter auch lohnt, diese sichere Art der Identifizierung in Online-Prozesse zu integrieren und neue Services bereitzustellen.

eID für eGovernment

Die Bundesregierung hat im Rahmen der Digitalen Agenda 2014-2017 daher beschlossen, die Nutzung des Personalausweises weiter zu vereinfachen und das Angebot zu erweitern, für welche Zwecke ihre Besitzer ihn nutzen können. So können heute etwa Steuererklärungen online (ELSTER) ausgefüllt und abgegeben oder alle ab dem

Person auf Grund einer Rechtsvorschrift festzustellen hat, einen elektronischen Identitätsnachweis mit dem Personalausweis oder dem elektronischen Aufenthaltstitel anzubieten“.
Auf der Seite des Bürgers werden auch die Client-Anwendungen kontinuierlich optimiert. So wird vom Bund nun eine zweite Generation der AusweisApp – die AusweisApp2 – angeboten. Ein besonderer Fokus liegt dabei auf der immer stärkeren Verwendung von mobilen Geräten. Zwar verfügen noch nicht alle genutzten Mobiltelefone über eine entsprechende NFC-Schnittstelle mit dem nötigen Funktionsumfang, doch ihre Zahl steigt stetig. Als mögliche

und alle dieselbe technische Hintergrundinfrastruktur nutzen. Dieser einheitliche Ansatz ermöglicht Flexibilität und schnelle Reaktionen auf politische Entwicklungen, wie zum Beispiel die aktuelle Flüchtlingssituation.

Ankunftsnachweis

Aufgrund der großen Zahl an Asylsuchenden, die im vergangenen Jahr nach Deutschland gekommen sind, arbeitet die Bundesregierung an einer Beschleunigung des Asylverfahrens. Am 9. Dezember 2015 hat die Bundesregierung daher einen Gesetzesentwurf zur Verbesserung der Registrierung und

Der papierbasierte Ankunftsnachweis gilt als Beleg der erfolgreichen Registrierung. Durch Sicherheitsmerkmale können Fälschungen besser vermieden werden.

des Datenaustauschs zu aufenthalts- und asylrechtlichen Zwecken beschlossen. Dieser Gesetzesentwurf hat zum Ziel, in Deutschland ankommende Asylsuchende möglichst gleich beim ersten Kontakt zu registrieren, sowie den Zugriff auf Daten und deren medienbruchfreien Austausch durch berechtigte Behörden zu verbessern. Auf diese Weise sollen Doppelregistrierungen vermieden und das weitere Asylverfahren in Zukunft beschleunigt werden.

Um die Identifizierung der Asylsuchenden zu verbessern, wird diesen in Zukunft von den Erstaufnahmeeinrichtungen oder den Außenstellen des Bundesamts für Migration und Flüchtlinge (BAMF) als Nachweis der erfolgreichen Registrierung ein Ankunftsnachweis ausgestellt. Hierbei handelt es sich um eine papierbasierte hoheitliche Bescheinigung. Der Einsatz moderner kryptografischer Verfahren stellt dabei sicher, dass die Daten auf dem Ankunftsnachweis echt sind und Fälschungen besser vermieden werden können. Der Ankunftsnachweis wird einen 2D-Barcode (Digitales Siegel) mit kryptografisch signierten Daten enthalten. Da der hierfür nötige Sicherheitsmechanismus auf dem technischen Familienkonzept hoheitlicher Dokumente basiert, war eine schnelle Einführung des Nachweises möglich. Zur Prüfung des 2D-Barcodes ist keine neue Hintergrundinfrastruktur notwendig, es werden die bewährten Systeme verwendet, welche für elektronische Reisepässe und Personalausweise bereits vorhanden sind.

eIDAS-Verordnung

Auch im Hinblick auf die grenzüberschreitende Verwendung von elektronischen Identitäten (eID) hat sich einiges getan. So wurde im Juli 2014 von der EU die Verordnung (EU) 910/2014 „über die elektronische Identifizierung und Vertrauensdienste für elektronische Transaktionen im Binnenmarkt“ verabschiedet.

Im Bereich eID basiert die Verordnung auf dem Prinzip der freiwilligen Notifizierung und der verpflichtenden gegenseitigen Anerkennung von notifizierten eID-Systemen, die zum 18. September 2018 beginnt. Zudem werden Vertrauensniveaus für eID-Systeme definiert und ein Interoperabilitätsrahmen für die grenzüberschreitende Verwendung geschaffen. Der Personalausweis erfüllt hierbei alle Voraussetzungen, um auf höchstem Vertrauensniveau notifiziert zu werden. ●

Dr. Guido Frank,
Referat eID-Technologien und Chipkarten


IT-Grund Schutz
De
De-Mail
SICHERHEITS LÜCKEN
CERT
Digi talisie rung
Stux net
CYBER SICHERHEIT
KRITISCHE INFRA STRUKTUR
eID
BSI FÜR BÜRGER
IT-SICHERHEIT
ALLIANZ FÜR CYBER SICHERHEIT
SAFER INTERNET DAY
KRYPTO GRAFIE
IT-SICHERHEITS GESETZ
1992
1993
1997
1998
1999
2003
2004
2011
2012

25 Jahre BSI

Mit Transparenz mehr Sicherheit

Genau wie die Informationstechnik (IT) eine noch vergleichsweise junge Technologie, ist das Bundesamt für Sicherheit in der Informationstechnik (BSI) eine noch vergleichsweise junge Behörde. Zum 1. Januar 1991 wurde es als Bundesoberbehörde aus der Taufe gehoben, mit dem BSI-Errichtungsgesetz vom 17.12. 1990 als gesetzlicher Basis und dem Bundesinnenminister als Taufpaten. Und genau wie die IT in den letzten 25 Jahren alle staatlichen, wirtschaftlichen und privaten Aktivitäten durchdrungen und das Internet die Kommunikation revolutioniert hat, sind die Aufgaben des BSI und die Bedeutung des Amtes gewachsen.

Die Anfänge

Bereits in den frühen 80er-Jahren wuchs bei Bundesregierung und Parlament die Erkenntnis, dass Informationstechnik anzuwenden auch heißt, das jeweils gebotene Maß an Sicherheit zu bedenken und zu realisieren. Und dass nur eine staatliche Stelle sowohl über die erforderlichen umfassenden Sicherheitsinformationen verfügen als auch Gewähr für ausreichende Neutralität bieten würde. Bis zu diesem Zeitpunkt war Sicherheitspolitik ein Synonym für territoriale Verteidigung, wurde Abwehr in der Zeit des „Kalten Krieges“ vor allem nachrichtendienstlich interpretiert.

Schon 1986 war der dem Bundesnachrichtendienst unterstellten Zentralstelle für das Chiffrierwesen (ZfCh) zusätzlich der Aufgabenbereich „Computersicherheit“ übertragen worden. 1989 wurde sie wegen der erweiterten Aufgabenstellungen in die Zentralstelle für die Sicherheit in der Informationstechnik (ZSI) umgewandelt. Aus ihr rekrutieren sich auch die Mitarbeiter des mit Gesetz vom 17.12.1990 neu gegründeten BSI, das dem Geschäftsbereich des Bundesinnenministeriums zugeordnet wird.

Die IT-Sicherheit erhält damit nicht nur eine gesetzliche Grundlage, sondern auch eine neue Ausrichtung. Dem Gesetz zugrunde liegen eine neue Definition von Sicherheit sowie ein neues Verständnis von Prävention und von Informationspolitik. Schon in dem von der Bundesregierung im Juni 1989 verabschiedeten Zukunftskonzept IT heißt es dazu: „Die Bundesregierung wird dafür sorgen, dass alle Betroffenen und Interessierten über Risiken, Schutzmaßnahmen und das Zusammenwirken verschiedener Stellen (Hersteller, Sicherheitsbehörden, Anwender) unterrichtet werden.“

Der Kerngedanke, dass ein Bundesamt für Sicherheit in der Informationstechnik über den staatlichen Geheimschutz hinaus für die IT-Sicherheit aller gesellschaftlichen Gruppen beratend und unterstützend tätig sein sollte, war damals durchaus nicht selbstverständlich: „Die Vorgänger-Behörde des BSI hatte ausschließlich für den staatlichen Sicherheitsbereich gearbeitet“, erinnerte sich BSI-Gründungspräsident Dr. Otto Leiberich (gest. 2015). „Nun kamen durch das BSI-Gesetz die IT-Sicherheit der Wirtschaft und der privaten Benutzer als Aufgabe hinzu. Die Übernahme dieser Aufgabe stellte eine große Herausforderung dar.“ Das BSI arbeitet ab jetzt operativ für die Verwaltung, kooperativ mit der Wirtschaft und informativ für den Bürger.

Die Aufgabenstellung

Doch spätestens mit Beginn der breiten Nutzung des Internets ab 1993 wurde deutlich, wie zukunftsweisend dieser Ansatz war. Durch die zunehmende Digitalisierung der gesamten Gesellschaft „entstanden völlig neue Bedrohungen, die Staat, Gesellschaft, Unternehmen und den Einzelnen betrafen“, resümiert rückblickend Dr. Dirk Henze, Präsident des BSI in diesen Jahren des digitalen Wandels (1993 – 2002). Die Sicherheit von IT-Systemen für die Funktionsfähigkeit von Wirtschaft und Staat gewann zunehmend an Bedeutung; Parallel dazu wurde das Thema „IT-Sicherheit“ nicht zuletzt durch Pannen und Pleiten bei der Nutzung von Online-Diensten wie dem „Millenium-Bug“ oder dem „LoveLetter“-Virus einer breiteren und beunruhigten Öffentlichkeit bekannt.

IT-Sicherheit wird nun zu einer vorrangigen staatlichen Aufgabe. Um sie zu schaffen und zu fördern, um ihre Bedrohung zu bekämpfen und zu mindern, muss der Staat immer stärker auch den zivilen, präventiven Bereich berücksichtigen, muss Rahmenbedingungen schaffen, Standards setzen und aktiv Hilfestellung geben. „Heute wird Computertechnologie überall eingesetzt, in privatwirtschaftlichen wie in behördlichen Prozessen“, meint Dr. Udo Helmbrecht, BSI-Präsident von 2003 – 2009. „Damit übernimmt der Staat auch Verantwortung für die IT-Sicherheit.“

Diese Erkenntnis ist damals weder selbstverständlich noch wird sie von allen gesellschaftlichen Gruppen geteilt. Die Diskussion um originäre staatliche Aufgaben auf dem Gebiet der IT-Sicherheit, um das Spannungsverhältnis zwischen Spähen und Sichern, begleitet das BSI seit seiner Gründung. Es führt dazu, dass es sich in einem kontinuierlichen Prozess von seinen traditionellen Aufgaben löst und zu einer unabhängigen und neutralen Stelle für Fragen zur IT-Sicherheit in der Informationsgesellschaft wandelt. Das BSI versteht sich nicht nur als kompetente Stelle für IT-Sicherheit, sondern auch als Institution, der im Handeln und Gestalten Vertrauen entgegengebracht werden muss. Und das nicht nur vom Staat und staatlichen Stellen, sondern von der

Öffentlichkeit und den Bürgern. Als Behörde ist es damit im Vergleich zu sonstigen europäischen Einrichtungen einzigartig.

Der IT-Sicherheitsdienstleister

Als nationale Sicherheitsbehörde ist es das Ziel des BSI, die IT-Sicherheit in Deutschland voranzubringen. Dabei ist es in erster Linie der zentrale IT-Sicherheitsdienstleister des Bundes. Dazu betreibt es seit 1994 ein Computer Emergency Response Team (CERT), das Informationen über Sicherheitslücken und neue Angriffsmuster sammelt, auswertet und Informationen und Warnungen an die betroffenen Stellen weitergibt: Operative Umsetzung der Erkenntnis, dass nicht nur die Abwehr von Schadprogrammen und der Hinweis auf Schwachstellen, sondern auch die Reaktion auf IT-Sicherheitsvorfälle wichtig sind.

Mit seinem Angebot wendet sich das BSI aber auch zunehmend an die Hersteller sowie die gewerblichen Nutzer und Anbieter von Informationstechnik. Mit dem IT-Grundschutz, mit der Common-Criteria-Zertifizierung und den Technischen Richtlinien trägt es dazu bei, dass sich das Verständnis für IT-Sicherheit und das IT-Sicherheitsniveau auch in der Privatwirtschaft erhöhen. Eine enge Zusammenarbeit mit allen Akteuren der IT- und Internetbranche auf dem Gebiet der IT-Sicherheit ist ein prioritäres Anliegen des BSI. So ist das Amt im Beirat des Vereins „Deutschland sicher im Netz e.V." vertreten und unterstützt das Anti-Botnet-Beratungszentrum des eco-Verbands der deutschen Internetwirtschaft e.V. Gleiches gilt für die 2012 gemeinsam mit dem Bundesverband Informationswirtschaft, Telekommunikation und neue Medien e.V. (Bitkom) gegründete „Allianz für Cyber-Sicherheit", in der aktuell 1473 Institutionen, über 93 aktive Partner und mehr als 41 Multiplikatoren auf freiwilliger Basis kooperieren. Seit 2007 arbeiten zudem das BSI und Betreiber der Kritischen Infrastrukturen in Deutschland auf Basis des Umsetzungsplans KRITIS eng zusammen, um neue Bedrohungen und Strategien zu diskutieren und Maßnahmen zu realisieren.

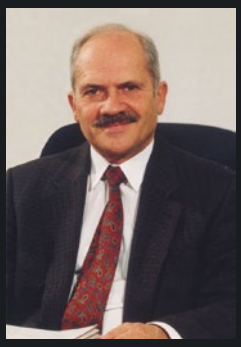
Ein weiteres Anliegen: Die Aufklärung und Sensibilisierung der privaten IT-Nutzer in Fragen der IT-Sicherheit. Dieser Aufgabe nimmt sich das BSI mit immer neuen Angeboten seit vielen Jahren an: Mit dem Informationsportal BSI für Bürger, mit dem Bürger-CERT, mit der BSI Facebook-Seite und dem BSI Service Center. Neben der reinen Information zu unterschiedlichsten IT-Sicherheitsthemen bietet das BSI über diese Kanäle auch konkrete Handlungsempfehlungen an.

Die Reform des BSI-Gesetzes

Mit der rasanten Fortentwicklung der Informationstechnik entstehen in fast allen Bereichen des Alltags neue IT-Anwendungen – und damit auch immer neue Sicherheitslücken. Das verlangt neue Antworten. Um den aktuellen IT-Bedrohungen begegnen zu können und der zunehmenden Bedeutung der Informations- und Kommunikationstechnologie Rechnung zu tragen, wurde das BSI-Gesetz 2009 durch das Gesetz zur Stärkung der Sicherheit in der Informationstechnik des Bundes novelliert – und machte das BSI endgültig zur nationalen IT- und Cyber-Sicherheitsbehörde. „Die Novellierung des BSI-Gesetzes 2009 war ein wichtiger Meilenstein für die zukünftige Entwicklung des BSI", so der damalige BSI-Präsident Helmbrecht.

Mit weitergehenden Befugnissen konnte das BSI nun neue Aufgaben angehen. Es entwickelte für die Bundesbehörden verbindliche Sicherheitsstandards für die Beschaffung und den Einsatz von IT. Mit der Übernahme der Aufgabe des Schutzes der Regierungsnetze wurde das BSI zentrale Meldestelle für IT-Sicherheit innerhalb der Bundesverwaltung. Hierdurch sollte auch bei IT-Krisen nationaler Bedeutung durch aufbereitete Informationen und kompetente Analysen die Entscheidungs- und Handlungsfähigkeit der Bundesregierung sichergestellt werden. Und es etablierte ein IT-Krisenmanagement für die Bundesverwaltung als eine Art Frühwarnsystem, das die Erstellung von Lagebildern ermöglicht, Krisenreaktionsprozesse definiert und mit Übungen unterlegt wird.

Daneben erhielt das BSI auch die Befugnis, Maßnahmen zum Schutz vor Gefahren für die Sicherheit der Informationstechnik des Bundes zu ergreifen. So darf es zur Sicherung der Regierungsnetze dort anfallende Daten erheben und auswerten. Soweit möglich, erfolgt die Auswertung dabei automatisiert und unterliegt strengen Kontrollen. Damit wird das BSI in die Lage versetzt, IT-Angriffe auf diese Netze zu erkennen und gezielt abzuwehren. ▶



01.01.1991
Gründung des BSI unter Dr. Otto Leiberich
Das BSI nimmt am 1.1.1991 seine Arbeit auf (BSI-Errichtungsgesetz). Gründungspräsident des BSI ist Dr. Otto Leiberich.

01.08.2001
Zentraler IT-Sicherheitsdienstleister des Bundes
Zum 1. August 2001 treten neue organisatorische, personelle und fachliche Rahmenbedingungen für die Weiterentwicklung des BSI zum zentralen IT-Sicherheitsdienstleister des Bundes in Kraft.

01.01.2000
Millenium-Bug
Die Angst vor Fehlfunktionen aufgrund des bisher üblichen zweistelligen Datumsformats, das nach dem Jahrtausendwechsel vierstellig sein musste, führt in der Bundesverwaltung zu eingehenden Analysen der IT-Systeme und massiven Vorbereitungen auf deren möglichen Ausfall. Das BSI übernimmt dabei die Federführung.

März 2002
BSI für Bürger
Der Informationsservice BSI-für-Bürger startet im März 2002 mit dem Slogan „Ins Internet – mit Sicherheit!“ als CD-ROM und steht seit 2003 als Internetangebot zur Verfügung.

1994
CERT
1994 wird das erste Computer Emergency Response Team (CERT) im BSI eingerichtet. Man hatte erkannt, dass nicht nur die Abwehr von Schadprogrammen und der Hinweis auf Schwachstellen, sondern auch die Reaktion auf IT-Sicherheitsvorfälle wichtig sind.

1990 1991 1992 1993 1994 1995 1996 1997 1998 1999 2000 2001 2002 2003 2004

01.01.1993
Präsident Dr. Dirk Henze
Dr. Dirk Henze wird zum BSI-Präsidenten bestellt.

04.05.2000
LoveLetter-Wurm
Schadsoftware rückt erstmals in das Bewusstsein der breiten Bevölkerung: Der Wurm „LoveLetter“ mit seiner verführerischen Betreffzeile („I love you“) verbreitet sich massenhaft per E-Mail und verursacht weltweit Schäden in Höhe von geschätzten 10 Milliarden Dollar.

01.03.2003
Präsident Dr. Udo Helmbrecht
Nach dem Ausscheiden von Dr. Dirk Henze im November 2002 wird Dr. Udo Helmbrecht im März 2003 zum BSI-Präsidenten bestellt.

1994
Einführung des IT-Grundschutz
In Kooperation mit führenden Wirtschaftsunternehmen konzipiert und veröffentlicht das BSI das IT-Grundschutzhandbuch, das sich in der Folge zu einem Standardwerk für das IT-Sicherheitsmanagement in Deutschland entwickelt.

01.11.2005
Elektronischer Reisepass
Der neu eingeführte elektronische Reisepass verfügt über einen integrierten Radio Frequency Chip, der das Gesichtsbild und die persönlichen Daten speichert, seit 1.11.2007 auch die Fingerabdrücke. Das BSI entwickelt entsprechende Protokolle und Technischen Richtlinien, die die Sicherheitsziele des elektronischen Reisepasses unterstützen: Datenschutz, Authentizität und Fälschungssicherheit.

20.08.2009
Novellierung BSI-Gesetz
Das Gesetz zur Stärkung der Sicherheit in der Informationstechnik des Bundes tritt in Kraft. Darin wird unter anderem geregelt, dass das BSI Informationen und Warnungen vor Sicherheitslücken in informationstechnischen Produkten und Diensten sowie vor Schadprogrammen an die betroffenen Stellen oder die Öffentlichkeit weitergeben darf. Insbesondere aber wird das BSI nun zentrale Meldestelle für die IT-Sicherheit der Bundesbehörden und damit verantwortlich für die Gewährleistung der Sicherheit der Informationstechnik des Bundes.

01.10.2011
Elektronische Gesundheitskarte
Mit der Gesundheitsreform 2004 beschließt der Gesetzgeber die Einführung der elektronischen Gesundheitskarte (eGK). Seit dem 1. Oktober 2011 geben die Krankenkassen schrittweise die neue Karte an ihre Versicherten aus. Die technischen Richtlinien des BSI und die Gewährleistung der IT-Sicherheit und der Vertrauenswürdigkeit technischer Komponenten durch Zertifizierung nach abgestimmten Schutzprofilen leisten einen wichtigen Beitrag zum hohen Sicherheitsstandard der eGK.

16.10.2009
Präsident Michael Hange
Michael Hange wird zum Präsidenten des BSI bestellt.

Nationales Cyber-Abwehrzentrum

01.04.2011
Cyber-Abwehrzentrum
Das Nationale Cyber-Abwehrzentrum in Bonn nimmt seine Arbeit auf. Unter der Federführung des BSI dient es mehreren Sicherheitsbehörden als gemeinsame Plattform zum schnellen Informationsaustausch und zur besseren Koordinierung von Schutz- und Abwehrmaßnahmen gegen IT-Sicherheitsvorfälle.

23.02.2011
Cyber-Sicherheitstrategie
Das Bundeskabinett beschließt die Cyber-Sicherheitsstrategie für Deutschland.

18.02.2016
Präsident Arne Schönbohm
Arne Schönbohm wird zum Präsidenten des BSI bestellt.

2005 2006 2007 2008 2009 2010 2011 2012 2013 2014 2015 2016 2017 2018

01.11.2010
Elektronischer Personalausweis
Mit dem elektronischen Identitätsnachweis macht es der neue Personalausweis möglich, sich im Internet gegenüber berechtigten Unternehmen und Behörden sicher und bequem auszuweisen. Das BSI etabliert die dafür nötigen Sicherheitsstandards und sichert die Qualität der technischen Prozesse.

06.06.2013
NSA-Affäre
Die Washington Post und der Guardian veröffentlichen geheime Dokumente, die belegen, dass amerikanische und britische Geheimdienste in großem Umfang die globale Telekommunikation und insbesondere das Internet überwachen. In der Folge wird öffentlich, dass auch deutsche Spitzenpolitiker abgehört wurden. Die dadurch ausgelöste „NSA-Affäre“ löst zahlreiche politische Diskussionen zu Cyber-Sicherheit und Geheimdienstpraktiken aus.

Juni 2010
Stuxnet
Mit Stuxnet wird erstmalig eine auf Prozesssteuerungssystem spezialisierte Schadsoftware bekannt. Damit rückt die Verwundbarkeit von Industrieanlagen und Kritischen Infrastrukturen in den Fokus.

Juli 2007
Zeus
Erstmals wird der Trojaner Zeus entdeckt, der vor allem zum Ausspähen von Privat- und Finanzdaten eingesetzt wird. Bis heute ist er einer der „erfolgreichsten“ Trojaner und hat in verschiedenen Varianten Millionen von PCs infiziert.

Allianz für Cyber-Sicherheit

08.11.2012
Allianz für Cyber-Sicherheit
In Zusammenarbeit mit dem Bundesverband Informationswirtschaft, Telekommunikation und neue Medien e.V. (Bitkom) gründet das BSI die Allianz für Cyber-Sicherheit. Als Zusammenschluss aller wichtigen Akteure im Bereich der Cyber-Sicherheit in Deutschland hat die Allianz das Ziel, die Cyber-Sicherheit in Deutschland zu erhöhen.

25.07.2015
IT-Sicherheitsgesetz
Als umfangreiche Ergänzung zum BSI-Gesetz tritt das „Gesetz zur Erhöhung der Sicherheit informationstechnischer Systeme (IT-Sicherheitsgesetz)“ in Kraft. Im Vordergrund steht die Stärkung der IT-Sicherheit bei Betreibern Kritischer Infrastrukturen.

Als schließlich die Bundesregierung 2011 – nicht zuletzt als Antwort auf den Angriff auf Prozesssteuerungssysteme durch die hochspezialisierte Schadsoftware Stuxnet – die Cyber-Sicherheitsstrategie verabschiedet und ein Cyber-Abwehrzentrum aufbaut, war es naheliegend, dass dies nur in Bonn und unter Federführung des BSI geschehen kann. Am 16. Juni 2011 wird das Nationale Cyber-Abwehrzentrum als gemeinsame Plattform zum schnellen Informationsaustausch und zur besseren Koordinierung von Schutz- und Abwehrmaßnahmen gegen IT-Sicherheitsvorfälle in den Räumen des BSI eröffnet. Das BSI, das Bundesamt für Verfassungsschutz und das Bundesamt für Bevölkerungsschutz und Katastrophenhilfe stellen die Mitarbeiter; seit Juni 2011 wirken als assoziierte Behörden auch das Bundeskriminalamt, die Bundespolizei, das Zollkriminalamt, der Bundesnachrichtendienst sowie die Bundeswehr mit.

Die Arbeit an Projekten

Die Möglichkeiten und Potenziale der IT und des Internets werden nur genutzt, wenn Vertrauen in die Sicherheit der Technik besteht. Qualitätssiegel von berufenen Stellen und etablierte IT-Sicherheitsstandards sind das Fundament für dieses Vertrauen. Mit Blick auf IT-Sicherheitsstandards bringt sich das BSI darum immer wieder in zukunftsweisende Projekte ein wie Smart Meter oder Cloud Computing. Im Bereich Smart Meter hat das BSI gemeinsam mit Wirtschaft, Daten- und Verbraucherschützern ein gemeinsames Schutzprofil und eine Technische Richtlinie erstellt. Auch beim Cloud Computing wurden gemeinsam mit Herstellern Mindestsicherheitsanforderungen erstellt und in einem Eckpunktepapier veröffentlicht.
Große Bedeutung hat auch die Mitarbeit und Mitgestaltung von gesellschaftlich relevanten Projekten, die die Bürger in ihrem Alltag betreffen, wie beispielsweise De-Mail und der neue Personalausweis. Die wesentlichen Sicherheitsziele Vertraulichkeit, Integrität und Authentizität bei der De-Mail-Kommunikation werden durch definierte Sicherungsmaßnahmen gewährleistet, an denen das BSI entscheidend mitgearbeitet hat. Mit dem neuen Personalausweis steht dem Bürger seit November 2010 nicht nur ein Sichtausweis im neuen Scheckkartenformat zur Verfügung. Das Ausweisdokument bietet zusätzlich verschiedene elektronische Funktionen, die auch im Internet für deutlich mehr Sicherheit sorgen. Dazu zählen der elektronische Identitätsnachweis und die qualifizierte elektronische Signatur.

Die Kritischen Infrastrukturen

Ein besonderes Augenmerk in der Zusammenarbeit mit der Wirtschaft liegt auf dem Schutz Kritischer Infrastrukturen, einer Gemeinschaftsaufgabe der Betreiber dieser Strukturen und des Staates. Ihr dient das im Juli 2015 verabschiedete IT-Sicherheitsgesetz, mit dem die Aufgaben und Verantwortlichkeiten des BSI erneut ausgeweitet werden. „Mit dem Gesetz wird die Rolle des BSI als zentrale Stelle für Belange der IT-Sicherheit für Wirtschaft und Gesellschaft gestärkt“, schätzt der ehemalige BSI-Präsident Michael Hange (2009 – 2015). „Und es kann seinen Beitrag zur Sicherung der Kritischen Infrastrukturen nunmehr auf einer sicheren gesetzlichen Grundlage leisten.“
Da die Kritischen Infrastrukturen für das Gemeinwohl unverzichtbar und immer stärker von IT abhängig sind, sollen sie künftig – genau wie die Bundesverwaltung – ein Mindestniveau an IT-Sicherheit einhalten und dem BSI IT-Sicherheitsvorfälle melden. Umgekehrt hat das BSI sämtliche für Abwehr von Angriffen auf die IT-Sicherheit Kritischer Infrastrukturen relevanten Informationen zu sammeln, zu bewerten und an die Betreiber sowie die zuständigen (Aufsichts-)Behörden weiterzuleiten.

Damit nimmt das BSI die 2009 für den Bereich der Bundesbehörden übernommene Rolle künftig auch für die Betreiber Kritischer Infrastrukturen wahr. Durch den im Gesetz verankerten kooperativen Ansatz profitieren nicht nur Staat und Wirtschaft vom Know-how des jeweils anderen, sondern der gesamtgesellschaftlichen Aufgabe größtmöglicher IT-Sicherheit kann so am besten Rechnung getragen werden.

Fazit: Das BSI hat sich in den letzten 25 Jahren zu einer operativ handelnden Behörde mit einer Zuständigkeit für die Informationssicherheit von Wirtschaft, Staat und Gesellschaft auf nationaler Ebene weiterentwickelt - und das mit Kompetenz auf allen Gebieten der IT-Sicherheit. Sein im BSI-Gesetz niedergelegter breiter Aufgabenkatalog und seine Befugnisse wecken aber zu Recht hohe Erwartungen, die die zukünftigen Herausforderungen nicht geringer werden lassen als die bei seiner Gründung.

25 Jahre BSI-Gesetz – die Entwicklung der Aufgaben und Befugnisse

1991: BSI-Errichtungsgesetz

Mit zunehmender Bedeutung aber auch Bedrohung der Sicherheit von IT-Systemen, die für Funktionsfähigkeit von Wirtschaft und Staat relevant sind, wurde als staatliche Aufgabe nicht mehr nur die Zulassung von Produkten für die Verarbeitung und Übertragung von Verschlusssachen gesehen, sondern auch das Ergreifen von Maßnahmen zur Verminderung der Bedrohung.

Das neu errichtete BSI sollte durch Untersuchung von Sicherheitsrisiken, Entwicklung von Sicherheitsvorkehrungen und Erteilung von Sicherheitszertifikaten einen staatlichen Beitrag zur Förderung der IT-Sicherheit leisten. Die Entwicklung entsprechender Prüfkriterien für Systeme und Komponenten sowie Beratung von Herstellern, Vertreibern und Anwendern informationstechnischer Systeme und Komponenten war ebenfalls Auftrag. Darüber hinaus sollte es sein informationstechnisches Know-how den Strafverfolgungs- und Verfassungsschutzbehörden zur Verfügung stellen, damit diese besser die aufkommende Cyber-Kriminalität bekämpfen können.

Das „Gesetz über die Errichtung des Bundesamtes für Sicherheit in der Informationstechnik“ war vom 01.01.1991 bis 19. August 2009 gültig.

2009: Novellierung des BSI-Gesetzes

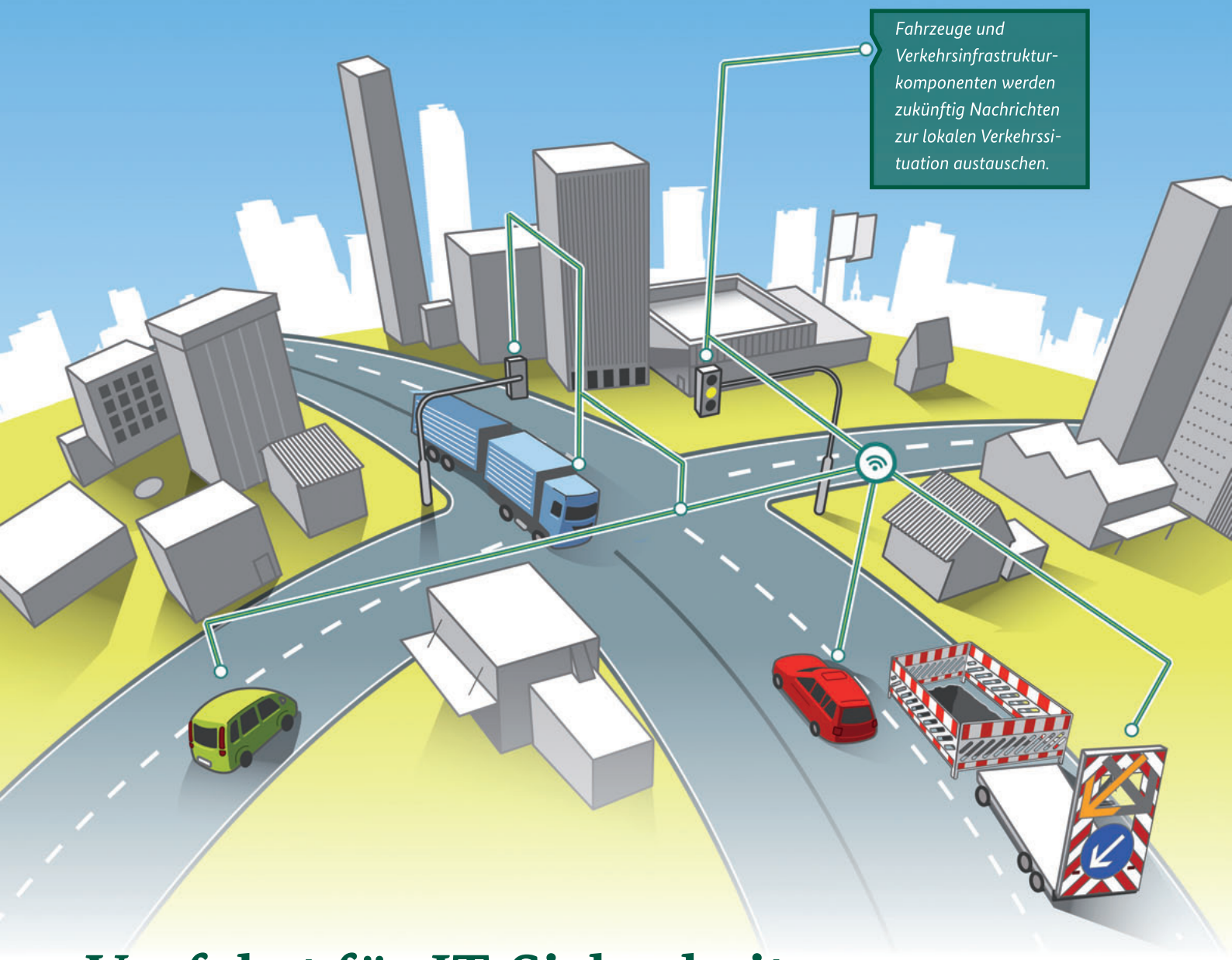
Einer der Schwerpunkte der Gesetzesnovellierung 2009 („Gesetz zur Stärkung der Sicherheit in der Informationstechnik des Bundes“) war die Verankerung des BSI als zentrale verantwortliche Stelle für die Gewährleistung der Sicherheit der Informationstechnik des Bundes. Mit dem am 20. August 2009 in Kraft getretenen Gesetz wurde das BSI zur zentralen Meldestelle für IT-Sicherheit für die Bundesbehörden. Es sammelt seither Informationen über Sicherheitslücken und neue Angriffsmethoden, die die Sicherheit der Informationstechnik gefährden, wertet diese aus und erstellt ein Lagebild. Angriffe auf die Bundesverwaltung können somit frühzeitig erkannt und Gegenmaßnahmen ergriffen werden. Über Warnungen darf das BSI auch betroffene Stellen außerhalb der Bundesverwaltung oder die Öffentlichkeit informieren.

Neben der Möglichkeit, technische Vorgaben für die Sicherung der Informationstechnik in der Bundesverwaltung zu erarbeiten, erhielt das BSI auch die Befugnis, Maßnahmen zum Schutz vor Gefahren für die Sicherheit der Informationstechnik des Bundes zu ergreifen. So darf das BSI zur Sicherung der Regierungsnetze dort anfallende Daten erheben und auswerten. Damit wird es in die Lage versetzt, IT-Angriffe auf diese Netze zu erkennen und gezielt abzuwehren.

2015: Ergänzung durch das IT-Sicherheitsgesetz

Da sich die Gefährdungen in kürzester Zeit von klassischen IT-Systemen auch auf Industriesysteme ausdehnten, stand bei der Novellierung 2015 („Gesetz zur Erhöhung der Sicherheit informationstechnischer Systeme“) die Stärkung der IT-Sicherheit bei Betreibern Kritischer Infrastrukturen im Vordergrund. Da diese gleichermaßen für das Gemeinwohl unverzichtbar und immer stärker von IT abhängig sind, sollen sie künftig ein Mindestniveau an IT-Sicherheit einhalten und dem BSI IT-Sicherheitsvorfälle melden. Umgekehrt sammelt das BSI sämtliche Informationen, die für Abwehr von Angriffen auf die IT-Sicherheit Kritischer Infrastrukturen relevant sind. Diese Informationen werden bewertet und an die Betreiber sowie die zuständigen (Aufsichts-)Behörden weitergeleitet.

Mit dem am 25. Juli 2015 in Kraft getretenen Gesetz nimmt das BSI die 2009 für den Bereich der Bundesbehörden übernommene Rolle künftig auch für die Betreiber Kritischer Infrastrukturen wahr.



Vorfahrt für IT-Sicherheit

Intelligente Verkehrssysteme

Europaweit werden die Weichen in Richtung automatisiertes Fahren gestellt. Ende April 2016 wird ein wichtiger Passus der Wiener Konvention von 1968 wegfallen, der den Einsatz autonomer Fahrfunktionen bislang verbot. Nach dem Übereinkommen zur Vereinheitlichung von Verkehrsregeln musste bislang ein Fahrer jederzeit sein Auto selbst führen und durfte die Hände deshalb auch nicht vom Steuer nehmen. Nun legt der Gesetzgeber vor und erlaubt den Herstellern und Zulieferern den Einsatz von Assistenzsystemen, die eigenständig das Fahrzeug lenken, die Spur halten und wechseln können und im Notfall auch das Auto abbremsen werden. Einzige Voraussetzung wird bleiben, dass der Fahrer jederzeit die Assistenzsysteme überstimmen und eingreifen kann. Jetzt sind also die Hersteller und Zulieferer am Zug, mit den schon weit entwickelten Assistenzsystemen künftig ihre Kunden mit zuverlässiger Funktion zu überzeugen. Bald wird es etwa neben den schon bekannten Notbremsassistenten mit Fußgängererkennung auch einen Ausweichassistenten geben. Vermutlich wird aber der Autobahnassistent als erstes System eingeführt, das in festgelegten Geschwindigkeitsbereichen die Fahrzeuge selbstständig in der Spur halten wird und in Gefahrensituationen das vollständige Abbremsen des Fahrzeugs übernimmt.

Schon in zehn Jahren könnte eine Fahrt vom Büro nach Hause wie folgt aussehen:
Über seine Smartphone Service-App hat der Autofahrer seine geplante Strecke, die er mit seinem Auto am Abend zurücklegen will, festgelegt. Sein Fahrzeug hat er morgens in dem in unmittelbarer Nähe seines Büros befindlichen Parkhaus abgegeben. Die pilotierte Parktechnologie seines Fahrzeugs macht es nicht mehr erforderlich, selbst einen Parkplatz zu suchen. Das übernimmt das Fahrzeug mittlerweile selbstständig. Die nicht unerhebliche Zeit, die früher alleine für die langwierige Parkplatzsuche angefallen ist, kann jetzt direkt als Arbeitszeit genutzt werden.
Die Positionsbestimmung seiner Service-App gibt dem Fahrzeug rechtzeitig den Hinweis, wann der Fahrer am vereinbarten Check-Out Punkt im Parkhaus ankommen wird. Das während der Parkdauer über Induktionsflächen automatisch aufgeladene E-Fahrzeug kommt zur gleichen Zeit am Check-Out Punkt an.

Für die Fahrt in der Stadt hat der Autofahrer entschieden, dass er sein Fahrzeug noch selbst steuern will. Erst auf der Autobahn will er sich entspannen und das Lenkrad loslassen können. Die seit wenigen Jahren mit intelligenten Kommunikationsmodulen ausgestatteten Verkehrsschilder helfen ihm mit Informationen zur Verkehrslage, die ihm in sein Fahrzeug in Echtzeit überspielte werden. Wie leicht ist es heute geworden, den schnellsten Weg aus der Stadt heraus zu finden. Kaum zu glauben, dass noch vor wenigen Jahren der Straßenverkehr mit überwiegend statischen Hinweisen geregelt worden ist. Auf der Autobahn angekommen, betätigt der Fahrer den Schalter für die Aktivierung des Autopiloten. Eine Anzeige im zentralen Display des Fahrzeugs zeigt an, dass alle Funktionen des Autopiloten verfügbar sind und einwandfrei arbeiten. Über Lenkradtaste bestätigt die Abgabe seiner Lenkaufgabe an den Autopiloten.

Alle Systeme im Fahrzeug arbeiten nun und bilden in Echtzeit mit Nahbereichsradar, Frontkamera und Fernbereichslaser- oder Radartechnologie ein genaues Abbild des Verkehrsgeschehens ab. Die metergenau verfügbaren Positionsdaten über die Galileo-Satelliten auf der einen Seite und der Abgleich der Sensoren mit den im Navigationssystem hinterlegten festen Objekten wie Leitplanken, Gebäude, Ampeln oder Bordsteinkanten auf der Fahrtroute andererseits ermöglicht es dem Fahrzeug, seine Fahrposition immer zentimetergenau selbst zu bestimmen. Alle diese festen Landschaftsobjekte sind als Daten in den neuen hochpräzisen Straßen- und Landschaftskarten im Navigationssystem des Fahrzeugs hinterlegt.

Sicher und entspannt das Fahrziel erreichen

Die Automatisierung der Fahrzeugführung soll sich nach den Plänen der Automobilwirtschaft bis voraussichtlich 2030 stufenweise von der Teilautomatisierung über die Hochautomatisierung, die Vollautomatisierung bis hin zum fahrerlosen, dem autonomen Fahrzeug, weiter entwickeln.

Bis aber die Zeit gekommen ist, dass alle Fahrzeuge fahrerlos gesteuert werden, wird es immer wieder Fahrsituationen geben, die das Fahrzeug noch nicht alleine bewältigen kann. So können beispielsweise besondere Gefahrensituationen nach Unfällen oder bei Schneefall eintreten. Können dann Fahrspuren nicht mehr zweifelsfrei erkannt werden, so wird das System die Steuerung mit einem rechtzeitig abgesetzten Warnsignal dem Fahrer übergeben.

Gefahren erkennen, bevor Sie zur Bedrohung werden

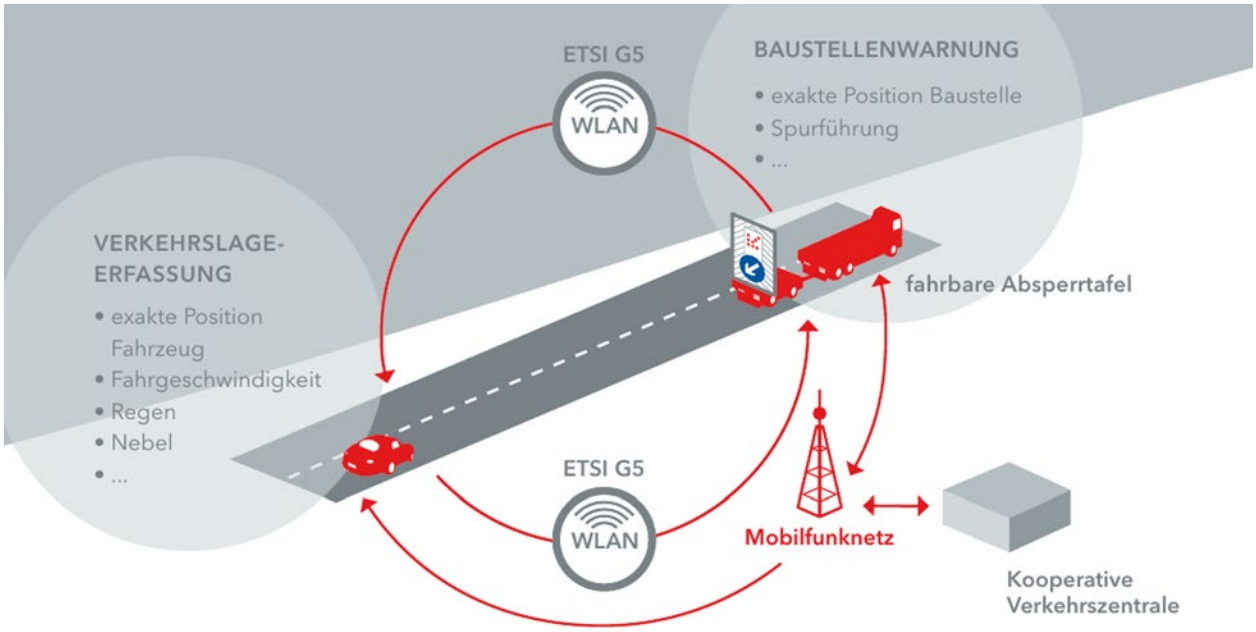
Einen weiteren wichtigen Baustein zum automatisiert fahrenden Fahrzeug stellen die aktuellen Entwicklungen zum vernetzten Automobil dar. Hierbei tauschen die Fahrzeuge per Funk untereinander und bald auch mit Verkehrsinfrastrukturkomponenten wie z.B. mit Straßenschildern oder Ampeln (Road Side Units) aktuelle Verkehrsinformationen aus. Der erste Fall wird als Fahrzeug-zu-Fahrzeug-, der zweite als Fahrzeug-zu-Infrastruktur-Kommunikation bezeichnet. Beides wird auch unter dem Begriff der Fahrzeug-zu-X-Kommunikation zusammengefasst. Durch rechtzeitiges Versenden von verkehrsrelevanten Informationen können Staus und Unfälle vermieden werden. Gerät etwa ein vorausfahrendes Fahrzeug in einen Stau oder muss aus anderen Gründen

bremsen, so wird an nachfolgende Fahrzeuge ein Datenpaket mit dieser Information verschickt, sodass deren Fahrverhalten (automatisch) entsprechend angepasst werden kann. Ziel des Austausches ist also die frühzeitige Information des Fahrzeugführers, bevor er diese Situation selber erkennt. Zukünftig werden diese Informationen auch dazu herangezogen, um das automatisierte Fahren zu unterstützen. Im Gegensatz zum autonom fahrenden Auto stehen vernetzt agierende Fahrzeuge kurz vor der Markteinführung.

Mit den neuen Kommunikationsmöglichkeiten werden allerdings bisher in sich geschlossen agierende Fahrzeuge nun weiter zur Außenwelt hin „geöffnet“ und damit auch einem möglichen Missbrauch durch potentielle Angreifer ausgesetzt. Bereits heute sind bestimmte Fahrzeugmodelle durch ihre Schnittstellen nach außen anfällig für Hackerangriffe, wie zahlreiche Veröffentlichungen in letzter Zeit gezeigt haben. Es war beispielsweise in einem Fall möglich, per Mobilfunkverbindung sogar in die Lenkung eines fahrenden Autos einzugreifen.

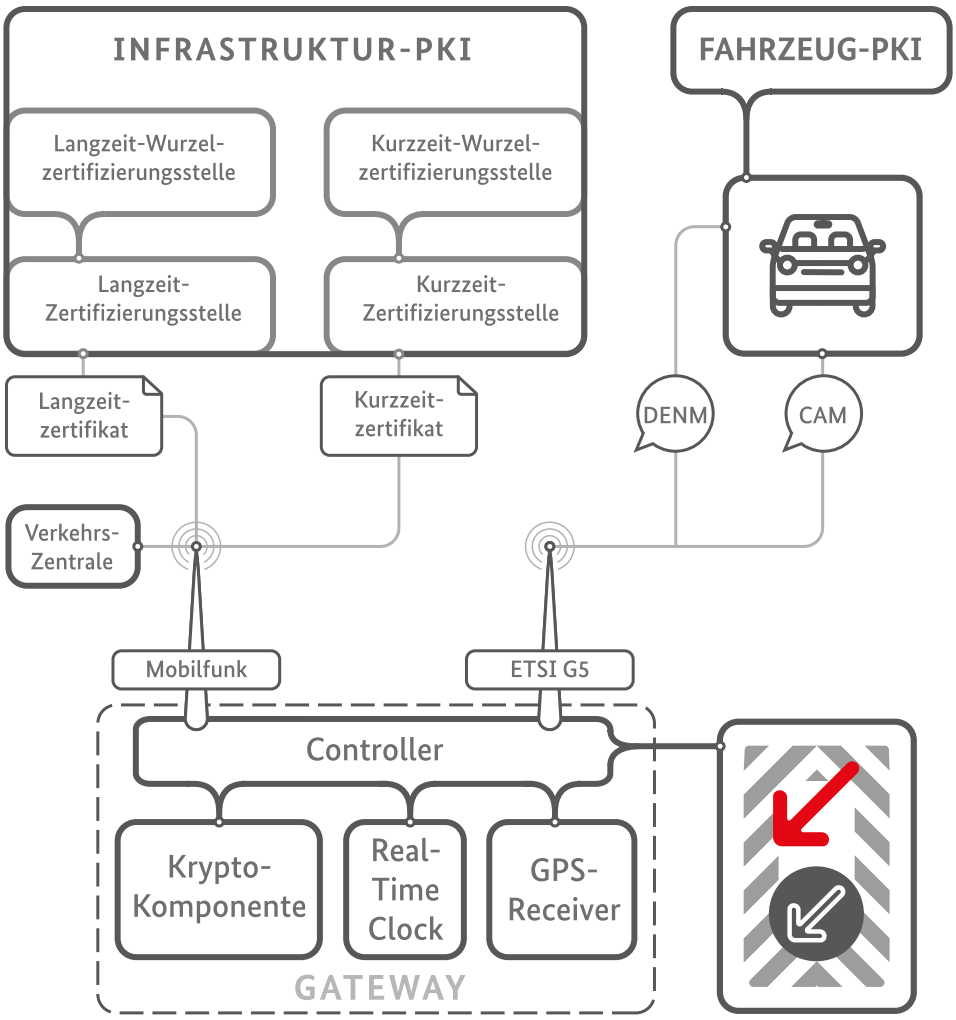
Auch für die Fahrzeug-zu-X-Kommunikation an sich sind Angriffe denkbar. Im dichten Autobahnverkehr könnte ein böswilliger Angreifer zum Beispiel gefälschte Nachrichten darüber verbreiten, dass bestimmte Fahrzeuge gerade scharf bremsen, sodass nachfolgende Fahrzeuge zu gefährlichen Bremsmanövern verleitet werden. Oder der Angreifer verschickt an einer Baustelle Meldungen, dass die linke Spur gesperrt ist, obwohl tatsächlich die rechte blockiert ist. Auf diese Weise könnten Verkehrsstörungen oder sogar Unfälle provoziert werden. Solche Angriffsmöglichkeiten müssen also verhindert werden, insbesondere muss die Integrität und Authentizität der ausgetauschten Nachrichten durch geeignete Verfahren sichergestellt werden. Zur Absicherung der Kommunikation zwischen Fahrzeugen und Verkehrsleitzentralen wird daher vom BSI die Entwicklung eines IT-Sicherheitskonzeptes für Infrastrukturkomponenten vorangetrieben.

Die Bundesregierung treibt das Thema Vernetzung der Fahrzeuge mit ihrem Engagement zum Aufbau einer intelligenten Verkehrsinfrastruktur voran. Ein erstes Anwendungsprojekt, in dem Fahrzeug-zu-X-Kommunikation in der Breite zum Einsatz kommt, ist das C-ITS-Korridorprojekt. Der C-ITS-Korridor wurde 2013 als länderübergreifendes Projekt von den Verkehrsministerien Deutschlands, der Niederlande und Österreichs initiiert. Im Rahmen dieses Vorhabens ist es geplant, einen Autobahnkorridor von Rotterdam über Frankfurt am Main bis Wien mit ersten intelligenten Verkehrssystemen auszustatten, die auf Fahrzeug-zu-X-Kommunikation zurückgreifen. Es werden hier zwei Dienste implementiert: Baustellenwarnung und Verkehrslageerfassung (siehe Abbildung). Eine zentrale Rolle werden dabei Baustellen-Warnanhänger spielen, die bei Tagesbaustellen und Wartungsmaßnahmen zum Einsatz kommen. Diese Baustellenwarner werden mit entsprechenden Gateways für die Kommunikation mit Fahrzeugen ausgerüstet. Auch zukünftig auf den Markt kommende Fahrzeugmodelle sollen geeignete Kommunikationskomponenten enthalten. Nähern sich nun die Fahrzeuge der Baustelle, so erhalten diese über



Die zwei Dienste Verkehrslageerfassung und Baustellenwarnung im C-ITS-Korridor. Daten werden über einen auf WLAN basierenden Kanal (ETSI G5) versendet.

Erste Anwendungsprojekte: Künftig sollen beispielsweise Baustellenwarner mit Gateways ausgestattet werden. Über die Datenverbindung zwischen Fahrzeug und Warnschild werden Informationen, wie gesperrte Spuren, Tempolimits beziehungsweise die aktuelle Fließgeschwindigkeit des Verkehrs ausgetauscht.



Aufbau der PKI für das Baustellenwarner-Gateway. Langzeit- und Kurzzeitzertifikate werden von verschiedenen Zertifizierungsstellen ausgestellt. Diese Instanzen sind wiederum jeweils an eine eigene Wurzelzertifizierungsstelle angebunden. Mit den Fahrzeugen tauscht das Gateway sogenannte Cooperative Awareness Messages (CAM) und Decentralized Environmental Notification Messages (DENM) aus. CAMs werden in kurzen Zeitabständen verschickt und enthalten Daten zum aktuellen Fahrzeugzustand wie etwa die Geschwindigkeit und Fahrtrichtung. DENMs entsprechen Warnmeldungen und werden nur in besonderen Verkehrssituationen, u.a. eben Baustellen, versendet.

das Gateway Warnmeldungen mit Informationen über gesperrte Spuren und Tempolimits, die im Fahrzeug per Display angezeigt werden. Der Fahrer kann so sein Fahrverhalten frühzeitig anpassen. Als weitere Funktion werden die Fahrzeuge selbst Nachrichten über ihren aktuellen Zustand (momentane Geschwindigkeit, Fahrtrichtung usw.) oder die unmittelbare Umgebung (z.B. Wetterbedingungen) versenden. Diese werden vom Baustellenwarner-Gateway empfangen und an eine Verkehrsleitzentrale weitergeleitet, wo diese Informationen zusammen mit bereits heute zur Verfügung stehenden Datenquellen in die Erstellung des Verkehrslagebildes einfließen.

Das zum Einsatz kommende Funknetzprotokoll und die Nachrichtenformate für die Fahrzeug-zu-X-Kommunikation wurden vom European Telecommunications Standards Institute (ETSI) standardisiert. Die Spezifikationen der ETSI sehen außerdem vor, dass Nachrichtenpakete zur Sicherstellung der Integrität und Authentitzität digital signiert werden. Es kommen dabei Signaturen auf Grundlage elliptischer Kurven (ECDSA) zum Einsatz. Hierzu muss eine geeignete Public-Key-Infrastruktur (PKI) aufgebaut werden, die die Zertifikate für die Signaturschlüssel der Fahrzeuge und der Baustellenwarner ausstellt und verwaltet. Das für das Projekt

verantwortliche Bundesministerium für Verkehr und digitale Infrastruktur hat das BSI frühzeitig für die Konzeption der PKI für Verkehrsinfrastrukturkomponenten wie den Baustellenwarner eingebunden. Das aktuell entwickelte Konzept basiert auf zwei Zertifikatstypen, Langzeitzertifikate und Kurzzeitzertifikate (Credential-Zertifikate). Unmittelbar nach der Produktion wird das Gateway im Baustellenwarner mit einem mehrere Jahre gültigen Langzeitzertifikat ausgestattet. Vor jedem geplanten Einsatz (etwa auf einer Tagesbaustelle) wird ein Kurzzeitzertifikat beantragt, dessen Gültigkeitszeitraum die Dauer der Baumaßnahme umfasst. Das Langzeitzertifikat dient dabei der Authentisierung gegenüber der Zertifizierungsstelle für die Kurzzeitzertifikate. Der zum Kurzzeitzertifikat gehörige Schlüssel wird zur Signierung der vom Gateway verschickten Warnmeldungen verwendet. Die kurze Gültigkeit reduziert das Angriffspotential im Falle einer Kompromittierung des Gateways, und es wird eine aufwändige Revokationsprüfung (also die Prüfung, ob ein Zertifikat für ungültig erklärt wurde) auf der Fahrzeugseite vermieden, die im Falle von länger gültigen Zertifikaten notwendig wäre.

Für die auf der Fahrzeugseite verwendeten Signaturschlüssel wird eine eigene PKI existieren. Es muss natürlich gewährleistet sein, dass Fahrzeuge und Verkehrsinfrastrukturkomponenten die jeweils empfangenen Signaturen und Zertifikate verifizieren können. Dazu muss beiden Seiten der öffentliche Schlüssel der Wurzelzertifizierungsstelle der jeweils anderen Seite zur Verfügung stehen.

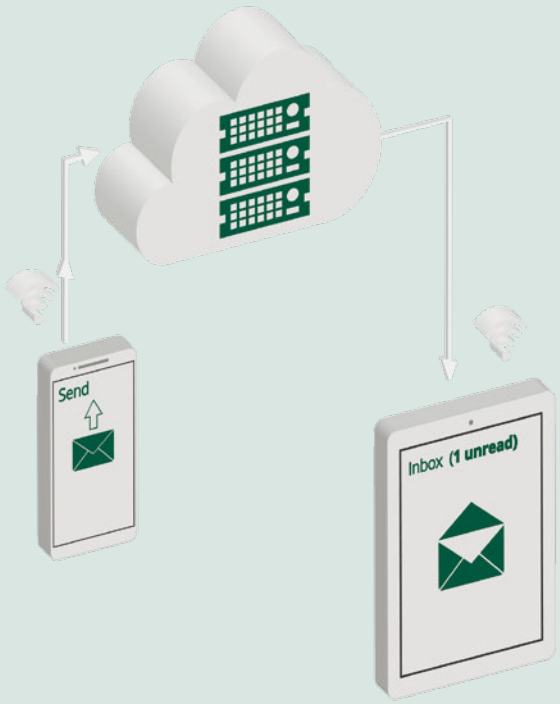
Die oben skizzierte PKI führt zu einem komplexen Schlüsselmanagement. Als Komponente, die die Authentizität von verkehrsbeeinflussenden Warnmeldungen kryptografisch sicherstellen muss, unterliegt das Gateway auf dem Baustellenwarnanhänger einem hohen Schutzbedarf. So darf es etwa einem Angreifer natürlich nicht möglich sein, den privaten Signaturschlüssel für ausgehende Nachrichten des Gateways auf irgendeine Weise auszulesen. Daher muss eine geeignete Hardwarekomponente eingesetzt werden, die eine sichere Speicherung privaten Schlüsselmaterials erlaubt. Auch müssen potentielle Angreifer daran gehindert werden, das Verhalten des Gateways etwa durch Manipulation der Soft- oder Firmware zu ändern. In Kooperation mit der Bundesanstalt für Straßenwesen (BASt) wird zurzeit ein Schutzprofil nach Common Criteria erstellt, das die Anforderungen an das Gateway beschreibt.

Das vernetzte Fahren wird sich natürlich nicht auf Deutschland beschränken. Die Vernetzungsfunktionen sollen grenzüberschreitend nutzbar sein, was eine internationale Harmonisierung der Systeme erfordert. Hierzu hat die EU-Kommission die sogenannte C-ITS-Plattform ins Leben gerufen, in der Fachleute in verschiedenen Arbeitsgruppen Handlungsempfehlungen für die Einführung intelligenter Verkehrssysteme auf europäischer Ebene ausgearbeitet haben. Danach ist auch im Bereich der IT-Sicherheit eine enge internationale Abstimmung erforderlich, da davon auszugehen ist, dass weiterhin nationale Public-Key-Infrastrukturen existieren werden, die interoperabel sein müssen.

Das vernetzte und autonome Fahren wird in den nächsten Jahren den Straßenverkehr deutlich verändern. Die Car-to-X-Kommunikation wird wie gesehen nicht auf die Interaktion mit Baustellenwarnern beschränkt bleiben. Vernetzte Fahrzeuge werden weiter in den Markt vordringen und weitere Verkehrsinfrastrukturkomponenten in der Fläche hinzukommen. Die IT-Sicherheit gewinnt also weiter an Bedeutung, auch die Absicherung der eingesetzten Hardware in Fahrzeugen und Road Side Units und den Schutz vor Hacking-Angriffen wird man in Zukunft noch stärker berücksichtigen müssen. Mit dem oben skizzierten Konzept sind aber hier die Grundlagen für einen sicheren Nachrichtenaustausch und vertrauenswürdige Verkehrsdienste auch im Hinblick auf das spätere automatisierte Fahren gelegt.

Christian Wieschebrink,
Referat Technologische Grundlagen sicherer elektronischer Identitäten, Chipsicherheit

Hans-Peter Wagner,
Referat Technologische Grundlagen sicherer elektronischer Identitäten, Chipsicherheit



Sicher kommunizieren im digitalen Zeitalter

Mit einer anwendungsorientierten Kombination von Maßnahmen in der Praxis

Die E-Mail bleibt trotz der wachsenden Bedeutung von mobilen Instant Messengern ein wichtiges Medium zum Austausch von Nachrichten in der digitalen Kommunikation. In der Regel werden E-Mails noch immer ohne die konsequente Anwendung von IT-Sicherheitsmaßnahmen wie Verschlüsselung und Signatur verschickt. Anders als bei geschlossenen Systemen hängt dies mit der heterogenen weltweit vernetzten IT-Landschaft zusammen, die beim Versand von E-Mails genutzt wird.

Das BSI hat sich mit der geplanten Technischen Richtlinie „Sicherer E-Mail-Transport (BSI TR-03108)“ vorgenommen, ein Mindestmaß an IT-Sicherheitsmaßnahmen für den Transport von E-Mails zu definieren und damit zur weiteren Verbreitung sicherer E-Mail-Technologien beizutragen. Dieses Vorhaben ist eine Ergänzung zu De-Mail und verschiedenen Projekten zur Förderung von Ende-zu-Ende abgesicherter digitaler Kommunikation. Die in der Technischen Richtlinie geforderten Maßnahmen zeichnen sich vor allem dadurch aus, dass sie ohne aktives Mitwirken der Nutzer wirken.

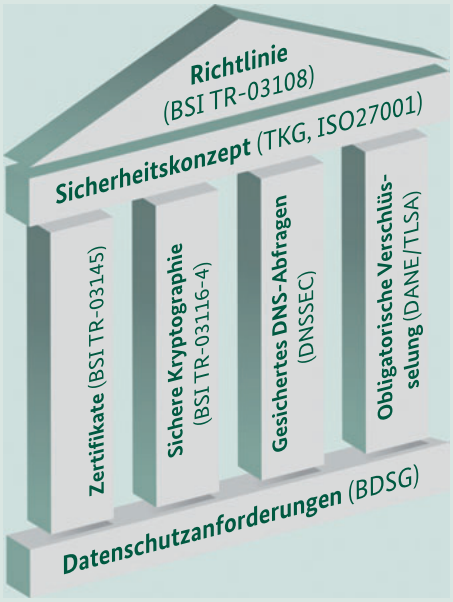
Der Bedarf nach einem transparenten sicheren E-Mail-Transport wurde schon früh von E-Mail-Diensteanbietern (EMDA) erkannt und am Markt adressiert. Ergänzend wünschten sich verschiedene Marktteilnehmer, dass das BSI einen Standard hierfür schafft. In Vorgesprächen wurden mögliche organisatorische und technologische Konzepte diskutiert. Ideen wurden erarbeitet, wieder verworfen oder verändert und weiterentwickelt. Am Ende stand ein tragfähiges Konzept, das konkrete Anforderungen an einen EMDA formuliert, um daraus einen Sicherheitsgewinn für alle Teilnehmer der E-Mail-Infrastruktur zu generieren. Hierzu werden in der Technischen Richtlinie Mindestanforderungen an den Betrieb, die Systeme und die Schnittstellen eines EMDA definiert. Vor der Einhaltung dieser Mindestanforderungen profitieren schließlich nicht nur die Nutzer des betreffenden EMDA, sondern auch die Nutzer anderer Anbieter, da die versendeten Nachrichten über sichere Verbindungen geschickt werden.

Praxiserprobte Lösungsansätze

Dieser Mehrwert ergibt sich vor allem aus der konsequenten Verwendung etablierter Standards. Neben BSI-eigenen Standards wie den Technischen Richtlinien zu kryptografischen Vorgaben für Projekte der Bundesregierung und zum sicheren Betrieb von Zertifizierungsstellen spielen in diesem Zusammenhang internationale Standards eine wichtige Rolle.

Besonders positiv wurde in der Öffentlichkeit die Verwendung von DNS-based Authentication of Named Entities (DANE) wahrgenommen. Dieser noch relativ junge Internet-Standard ermöglicht es Internet-Diensteanbietern, ihre für die Authentisierung und Verschlüsselung notwendigen Zertifikate durch die Veröffentlichung auf DNS-Servern bekannt zu machen. In der analogen Welt ist das vergleichbar mit dem Hinterlegen öffentlicher Schlüssel in einem Telefonbuch. Auf diese Weise kann jeder, der Kontakt mit einem Diensteanbieter aufnehmen möchte, dies auf verschlüsseltem Weg tun. Tatsächlich geht DANE an dieser Stelle noch einen Schritt weiter, denn seine Nutzung ist gleichzeitig ein Statement, dass der Diensteanbieter standardmäßig in der Lage ist, eine verschlüsselte Verbindung anzubieten. Damit ist DANE eine Technologie, die obligatorisch sichere Verbindungen skalierbar in die Fläche bringt. Das BSI selbst bietet seine Dienste bereits seit einiger Zeit mit DANE im Internet an.
Internetverbindungen, die mithilfe von

Transport Layer Security (TLS) abgesichert werden, finden im Gegensatz zu DANE schon seit einiger Zeit in der Praxis zunehmende Verbreitung. Sicherheitsschwächen wie der Trojaner BEAST oder die Man-in-the-middle-Attacke Poodle haben in jüngster Vergangenheit gezeigt, dass vor allem der Einsatz zeitgemäßer Kryptoverfahren von essenzieller Bedeutung ist. Das BSI veröffentlicht aus diesem Grund jährlich und anlassbezogen neue Sicherheitsvorgaben, die ebenfalls beim sicheren E-Mail-Transport angewandt werden. Durch die Kombination der Internetstandards DNSSEC zur sicheren Abfrage beim DNS-Server, DANE zum Abruf von Zertifikatsinformationen und den Einsatz von sicheren Algorithmen bei TLS wird mithilfe von Standardtechnologien ein einheitlich hohes Sicherheitsniveau erreicht.



Konzeptionelle Übersicht der Anforderungen

Um die gesamte Strecke vom Sender bis zum Empfänger einer E-Mail von Punkt-zu-Punkt abzusichern, genügt es jedoch nicht, nur Anforderungen an die Schnittstellen zu definieren. Jeder EMDA bildet einen Punkt in der Infrastruktur, der – je nach der Route einer E-Mail – diese auf ihrem Weg verarbeitet. Daher benötigt ein EMDA auch einen sicheren Betrieb. Die Technische Richtlinie formuliert deshalb Anforderungen an das vom EMDA zwingend zu erstellende Sicherheitskonzept. Kombiniert mit den hohen Datenschutzanforderungen zum Betrieb des E-Mail-Dienstes wird so die gesamte Strecke, die eine E-Mail zwischen Sender und Empfänger zurücklegt, abgedeckt.

Jeder E-Mail-Diensteanbieter soll in Zukunft auch die Möglichkeit erhalten, die Konformität seines Dienstes zu der Technischen Richtlinie im Rahmen eines Zertifizierungsverfahrens nachzuweisen. Ein entsprechendes Zertifizierungsschema wird derzeit erarbeitet. Durch die Zertifizierung erhält der Diensteanbieter von einer unabhängigen Stelle den Nachweis darüber, dass er ein definiertes Sicherheitsniveau umgesetzt hat. Dies dient der Abgrenzung gegenüber anderen Marktteilnehmern, aber auch der Transparenz gegenüber den Nutzern.

Im Gegensatz zu diesen, flächendeckend greifenden/systemübergreifenden Maßnahmen, die der Schaffung eines vergleichbaren Sicherheitsniveaus in einer offenen Infrastruktur dienen, werden mit anderen Vorhaben wie De-Mail in sich geschlossene Infrastrukturen geschaffen. Diese erlauben konkrete Aussagen in Bezug auf das Sicherheitsniveau jeder einzelnen über diese Infrastruktur versendeten Nachricht. Auf diese Weise lassen sich Verbindlichkeiten schaffen, die eine digitale Kommunikation erlauben, welche unter bestimmten Voraussetzungen sogar den Anforderungen entspricht, welche geeignet sind die klassische Schriftform zu ersetzen. Die beiden Vorhaben decken somit sich ergänzende Anwendungsbereiche ab.

Unabhängig von der Infrastruktur zum Transport einer Nachricht fördert das BSI aktiv Projekte zur Umsetzung von Sicherheit, die Ende-zu-Ende umgesetzt wird. Diese Verfahren finden aktuell noch keine breite Anwendung. Ein Grund hierfür könnte in einer als zu gering empfundenen Nutzerfreundlichkeit liegen, beispielsweise durch das in der Regel komplexe und aufwendige Schlüsselmanagement. Aktuelle Projekte setzen an genau dieser Stelle an und zielen darauf ab, den Nutzern ein möglichst automatisiertes und damit bedienfreundlicheres Verfahren zu bieten. Sowohl De-Mails als auch reguläre E-Mails lassen sich mittlerweile auf deutlich vereinfachte Weise Ende-zu-Ende-abgesichert übertragen und erreichen so für Nutzer ein sichtbar hohes Niveau an Vertraulichkeit.

Letzten Endes bestimmt nicht nur die Kombination von Maßnahmen innerhalb eines Projektes, den Erfolg von sicherer digitaler Kommunikation , sondern auch das Zusammenspiel von Projekten, die sich in ihrer Anwendung ergänzen. ●

Florian Bierhoff,
Referat Sicherheit in eID-Anwendungen

Der neue Präsident des BSI

Arne Schönbohm tritt sein Amt an

Bei der Verabschiedung des bisherigen BSI-Präsidenten Michael Hange gab Bundesinnenminister Dr. Thomas de Maizière am 11. Dezember 2015 bekannt, dass er Arne Schönbohm, zu diesem Zeitpunkt Präsident des Cyber-Sicherheitsrates e.V., als künftigen Präsidenten des BSI vorschlagen wird. Nach der Bestätigung durch das Bundeskabinett hat Schönbohm am 18. Februar 2016 sein neues Amt angetreten.

Vor seiner Ernennung zum BSI-Präsidenten war Arne Schönbohm mehr als drei Jahre als Präsident des im August 2012 gegründeten Cyber-Sicherheitsrats Deutschland e.V. tätig. Der in Berlin ansässige Verein ist politisch neutral und hat sich zum Zweck gesetzt, Unternehmen, Behörden und politische Entscheidungsträger im Bereich Cyber-Sicherheit zu beraten und im Kampf gegen die Cyber-Kriminalität zu stärken. Zu den Mitgliedern des Vereins zählen große und mittelständische Unternehmen, Betreiber Kritischer Infrastrukturen (KRITIS), Bundesländer, Kommunen sowie Experten und politische Entscheider mit Bezug zum Thema Cyber-Sicherheit.

Parallel zu dieser Tätigkeit war Arne Schönbohm bereits seit Ende 2008 Vorstandsvorsitzender der BSS BuCET Shared Services AG (BSS AG), die Unternehmen und Behörden in den Bereichen Digitalisierung, Cyber-Sicherheit und Datenschutz berät. Zum Portfolio der BSS AG gehören darüber hinaus Beratungsleistungen für die Bereiche Public Affairs und Public Relations, um digitale Themen und Meldungen professionell und sachverständig zu kommunizieren. In beiden Funktionen hat Arne Schönbohm als national und international gefragter Experte und Redner in zahlreichen Publikationen und im Rahmen von Medienauftritten zu den Themen Cyber-Kriminalität und Cyber-Sicherheit Stellung genommen.

Besonderes Augenmerk lag hierbei vor allem auf der Vernetzung und Beratung auf der Entscheiderebene, als Schlüsselebene im Kampf für weltweite Cyber-Sicherheit. So war Arne Schönbohm u.a. in den USA Vortragender auf Veranstaltungen der National Association of Corporate Directors (NACD) oder als Sachverständiger bei Anhörungen im Landtag von Nordrhein-Westfalen oder im Abgeordnetenhaus von Berlin tätig. Zudem ist er Autor diverser Bücher, darunter des Buches „Deutschlands Sicherheit – Cybercrime und Cyberwar (2011)“.

Der in Hamburg geborene Arne Schönbohm (Jg. 1969) legte im Jahre 1989 das Abitur am Gymnasium Röttgen im Rheinland ab. Nach dem Wehrdienst studierte er internationale Betriebswirtschaftslehre an der International School of Management in Dortmund sowie in London und Taipei und erwarb im Jahre 1995 den Abschluss als Diplom-Betriebswirt (FH).

Seine 13-jährige Industriekarriere begann Schönbohm als Trainee in der zentralen Nachwuchsgruppe bei DaimlerChrysler Aerospace in München.

Arne Schönbohm,
Präsident des Bundesamts für Sicherheit in der Informationstechnik

Nach Abschluss der Traineezeit arbeitete er als Sachbearbeiter in der strategischen Unternehmensentwicklung der Motoren- und Turbinen-Union (MTU) und als Leiter des Vorstandsbüros. Nach der Gründung der EADS wechselte er als Senior Manager Telecom im September 2001 zu EADS Defence and Civil Systems. 2003 ging er als Mitglied der Geschäftsleitung für die Bereiche Public Affairs and Homeland Security bei der EADS Telecom Deutschland GmbH nach Ulm. 2005 kehrte Schönbohm nach München zurück, wo er die Verantwortung für das Strategie- und Business-Development der EADS Secure Networks übernahm und als Board-Mitglied tätig war. 2006 stieg er in die Position des Vizepräsidenten für Commercial und Defence Solutions auf. Dort war er zuständig für den Aufbau und die Führung dieses internationalen Geschäftsfelds und gewann insbesondere die Streitkräfte und KRITIS-Betreiber wie Energieversorger, Flughäfen und den öffentlichen Personennahverkehr als Kunden für die EADS Secure Networks. Seit Dezember 2012 ist Schönbohm Mitglied der Cyber Security Coordination Group.

Einladung in die Werkstatt

Neues Format des Mediendialogs

Wer Journalisten für seine Arbeit interessieren will, muss ihnen etwas bieten können. Das sind natürlich in erster Linie nutzbare, wertige Inhalte, jedoch spielt durchaus auch die Form der Präsentation eine Rolle. Das BSI hat sich deshalb das neue Format „Werkstattgespräch" für die Kooperation mit den Medien eingeführt. Journalisten erhalten einen vertieften Einblick in die Arbeit des BSI, lernen Personen, aber auch Produkte kennen und können im Gespräch ihre Fachfragen platzieren. Am 29. Oktober 2015 wurde dieses Format erstmals erfolgreich umgesetzt.

Als nationale IT- und Cyber-Sicherheitsbehörde ist es Aufgabe des BSI, die Sprach- und E-Mail-Kommunikation der Regierung und der Bundesverwaltung mittels Kryptografie und sicherer Geräte zu schützen. Dazu zählt auch, in Zusammenarbeit mit den jeweiligen Herstellern Kommunikationslösungen für den Einsatz in der Bundesverwaltung bereitzustellen und diese für deren Anwendung zu sensibilisieren.
Aus diesem Grund wurde bereits im Jahr 2012 eine Ausschreibung sicherer mobiler Kommunikationsgeräte für die Bundesverwaltung vorgenommen. Aufgabe des BSI war es dabei, die Anforderungen zu definieren, die ausgewählten Geräte zuzulassen und eine Kommunikationsplattform für den Erfahrungsaustausch bereitzustellen. Für das BSI wie für die Hersteller war diese Ausschreibung mit der Herausforderung verbunden, einen für alle Seiten tragbaren Kompromiss zwischen Sicherheit, Benutzbarkeit und Preis zu finden.
Verschlüsselung ist angewandte Spionageabwehr. Das macht sie aus journalistischer Sicht zu mehr als einem IT-fachlichen Thema. Zu Recht, schließlich geht es um den Schutz der Regierungskommunikation. Aber sichere mobile Kommunikation ist auch ein Thema, das Journalisten mit einem hohen Eigeninteresse verfolgen. Denn die journalistische Recherche und der stabile Schutz von Informanten sind in der Regel untrennbar damit verbunden, sicher mobil kommunizieren zu können.
Kryptografie ist ein komplexes technisches Fachgebiet, was die journalistische Darstellung nicht gerade vereinfacht, vor allem, wenn nicht IT-Fachjournalisten, sondern Redakteure der Ressorts Politik und Gesellschaft sich damit auseinandersetzen. Im Werkstattgespräch sollte den Hauptstadtjournalisten daher vermittelt werden, was das BSI mit Kryptografie meint und welche Krypto-Lösungen für welche Arten von Kommunikation, Einsatzbereiche und Nutzergruppen bereitstehen und geeignet sind. Dafür stellten sich als kompetente Gesprächspartner Dr. Gerhard Schabhüser, Abteilungsleiter Krypto-Technologie im BSI, Dr. Uwe Kraus, Fachbereichsleiter VS-IT-Sicherheit, Vorgaben an und Zulassungen von Krypto-Systemen im BSI, und Clemens Taube, BSI-Referent zum Thema Kryptografie in Anwendungen, zur Verfügung.
Nach einem Impulsreferat von Dr. Schabhüser zu Elementen und Grundzielen der Kryptografie, Arten der Verschlüsselung sowie Schlüsselmanagement und -verteilung informierte Dr. Kraus über die Technische Richtlinie „Kryptografische Verfahren" und präsentierte verschiedene Krypto-Lösungen. Von den Journalisten wurden zahlreiche Fragen sowohl zu politischen als auch zu technischen Aspekten des Themas gestellt. Dies verdeutlicht, dass auch für Journalisten nicht nur die Technikperspektive, sondern vor allem auch die Anwenderperspektive eine gewichtige Rolle spielt. Neben die Frage, was technisch möglich ist, tritt gleichberechtigt die Frage, wie das technisch Mögliche in die beruflichen Alltagsabläufe passt. Denn es gilt: Die passgenaue Übereinstimmung beider Perspektiven entscheidet über den Erfolg der eingesetzten Schutzmechanismen. Und das nicht nur bei Bundesbehörden, sondern gleichfalls in der Wirtschaft sowie in den Medien.
Die Werkstattgespräche des BSI mit Journalisten sollen nach diesem gelungenen Auftakt auch 2016 fortgeführt werden. ●

Innovativ und nah am Alltagsleben

Das BSI als Arbeitgeber

Thomas Gilles arbeitet als Referent für Sicherheit in eID-Anwendungen beim BSI. Im Interview berichtet er über seinen Einstieg als Bachelorand und warum er sich für die Arbeit im öffentlichen Dienst entschied.

Thomas Gilles,
Referat Sicherheit in eID-Anwendungen

Seit wann genau arbeiten Sie für das BSI und wie sind Sie eingestiegen?

Vor fast zehn Jahren habe ich im BSI angefangen und habe seitdem verschiedene Positionen durchlaufen. Begonnen habe ich 2006 als Werkstudent, indem ich meine Bachelorarbeit im BSI geschrieben habe. Danach habe ich eine unbefristete Stelle als Sachbearbeiter im gehobenen Dienst erhalten und wurde 2009 auf dieser Stelle verbeamtet. Anschließend habe ich ein Masterstudium absolviert und mich 2011 mit Erfolg auf eine Referentenstelle beworben.

Wie sieht Ihre Tätigkeit aus und was umfasst sie?

Ich arbeite im Referat „Sicherheit in eID-Anwendungen“ und beschäftige mich dort vor allem mit der Konzeption und Umsetzung von eID-Infrastrukturen. Dazu gehört zum Beispiel die Smart-Metering-Public-Key-Infrastruktur (PKI), mit der die Daten vernetzter Stromzähler sicher übermittelt werden können. Ein weiteres Arbeitsgebiet ist die Nutzung der Online-Ausweisfunktion des Personalausweises zur Ableitung anwendungsbezogener elektronischer Identitäten. Insgesamt entwickle und bewerte ich technische Konzepte und Standards und betreue Projekte, um diese in Anwendungen umzusetzen.

Was hat Sie damals dazu bewogen, sich beim BSI zu bewerben?

Mein Interesse für die IT-Sicherheit war schon früh vorhanden und wurde im Studium durch die Wahl meiner Vorle-

sungen gestärkt. Während ich meine Bachelorarbeit geschrieben habe, wurde ich in meinem Wunsch bekräftigt, im BSI zu arbeiten. Ich habe mich direkt nach meiner Abschlussarbeit beworben und hatte das Glück, eine unbefristete Stelle zu erhalten.

Wie kam es dazu, dass Sie Ihre Bachelorarbeit im BSI geschrieben haben, und wie genau lief das ab?

Auf das BSI bin ich zunächst einmal durch den mittlerweile pensionierten Kollegen Marcel Weinand aufmerksam geworden. Zu der Zeit war er Dozent im Bereich Common Criteria an der Hochschule Bonn-Rhein-Sieg, an der ich studierte. Er bot mir die Chance, beim BSI meine Bachelorarbeit zu schreiben. Darüber bin ich rückblickend sehr froh.
Ich bekam einen Büroarbeitsplatz im BSI und konnte mich hier mit den Kollegen austauschen. Dabei habe ich die tägliche Arbeit und speziell das Arbeitsklima vor Ort erlebt, was mir nicht nur bei meiner Bachelorarbeit geholfen hat, sondern mir auch die Entscheidung erleichterte, was ich nach dem Abschluss machen und wo ich arbeiten möchte.

Thema meiner Abschlussarbeit war übrigens die Entwicklung eines Sicherheitsstandards für USB-Datenträger. Es ist schön zu erleben, dass dieser Standard mittlerweile tatsächlich bei Produkten angewendet wird.

Welche Aufstiegsmöglichkeiten bietet das BSI einem Absolventen mit Bachelorabschluss?

Die Hochschulabschlüsse Bachelor und Master bilden die Grundlage für jeweils unterschiedliche Laufbahnen, den gehobenen und den höheren Dienst. In der Regel findet der weitere Aufstieg dann innerhalb dieser Laufbahnen statt.
Ich habe parallel zu meiner Arbeit noch ein Fernstudium mit Masterabschluss absolviert, der mir dann die Möglichkeit eröffnete, mich auf eine Referentenstelle zu bewerben und in die Laufbahn des höheren Dienstes zu wechseln.

Was zeichnet das BSI als Arbeitgeber aus, was macht es besonders hier zu arbeiten, auch im Gegensatz zu einer Stelle in der freien Wirtschaft?

Was ich besonders an der Arbeit im BSI schätze, ist, dass ich mich immer mit aktuellen und sehr innovativen Themen beschäftige. Langweilig war es hier noch nie. Als Berufseinsteiger bin ich gut aufgenommen worden und konnte schnell Praxiserfahrung sammeln.
Da ich in der freien Wirtschaft noch nie gearbeitet habe, kann ich keine Vergleiche ziehen. Grundsätzlich sehe ich es aber als Vorteil, dass man sich hier wirklich darauf konzentrieren kann, seine Themen inhaltlich voranzubringen, weil eben nicht der wirtschaftliche Erfolg im Vordergrund steht.

Beamter im öffentlichen Dienst gilt aber oft nicht gerade als innovativ, oder?

Beamter zu sein tut nicht weh. Ein sicherer Arbeitsplatz ist eine feine Sache, auf der man viel aufbauen kann. Das BSI ist auch keine klassische Verwaltungsbehörde, sondern ein technischer Dienstleister. Hier kann man viel voranbringen. Im Laufe der Jahre habe ich an mehreren Großprojekten des Bundes mitgearbeitet, zum Beispiel am elektronischen Reisepass und Personalausweis sowie im Smart Metering. Es ist schön, wenn die eigene Arbeit einen starken Bezug zum Alltagsleben hat und man ihre Ergebnisse genau dort wiederfindet: etwa als Ausweiskarte im Portemonnaie. ●

Das BSI als Arbeitgeber

Zur Zeit beschäftigt das BSI rund 600 Mitarbeiterinnen und Mitarbeiter, größtenteils mit einem abgeschlossenen Hochschul- oder Fachhochschulstudium der Ingenieurwissenschaften, Mathematik, Informatik oder Physik.
Team- und Projektarbeit wird im BSI besonders gefördert, um flexibel auf die technischen Herausforderungen reagieren zu können. Ziel ist es, auf dem Gebiet der IT-Sicherheit immer einen Schritt voraus zu sein. Die Bereitschaft der Mitarbeiterinnen und Mitarbeiter, die bestehenden guten Fortbildungsmöglichkeiten zu nutzen, ist hierfür Voraussetzung.

Informationen über das BSI als Arbeitgeber, aktuelle Stellenanzeigen und Infos zu Ausbildung, Studienförderung und Diplomarbeiten finden Sie unter: www.bsi.bund.de/jobs

Impressum

Herausgeber:	Bundesamt für Sicherheit in der Informationstechnik (BSI), 53175 Bonn
Bezugsquelle:	Bundesamt für Sicherheit in der Informationstechnik (BSI) Referat B23 – Öffentlichkeitsarbeit und Presse, Godesberger Allee 185–189, 53175 Bonn Telefon: +49 (0) 22899 9582-0, E-Mail: oeffentlichkeitsarbeit@bsi.bund.de, Internet: www.bsi.bund.de
Stand:	März 2016
Texte und Redaktion:	Stephan Kohzer und Nora Basting, Bundesamt für Sicherheit in der Informationstechnik (BSI); Joachim Gutmann, GLC Glücksburg Consulting AG
Konzept, Redaktion und Gestaltung:	Fink & Fuchs Public Relations AG (FFPR), Berliner Straße 164, 65205 Wiesbaden, Internet: www.ffpr.de
Druck:	Druck- und Verlagshaus Zarbock GmbH & Co KG, Sontraer Str. 6, 63086 Frankfurt a.M., Internet: www.zarbock.de
Artikelnummer:	BSI-Mag 16/703-1
Bildnachweis:	Titel: Fink & Fuchs Public Relations AG; S. 4: Jordan Tan/Shutterstock (o.l.), Ed Gregory/pexels.com (o.r.), Fink & Fuchs Public Relations AG (m.), Matej Kastelic/Shutterstock (u.l.), Fink & Fuchs Public Relations AG (u.r.); S. 8: Pressestelle Airbus Group; S. 9: Jordan Tan/Shutterstock; S. 10: Pressestelle Airbus Group; S.13: Idealistock/iStock; S.16: Anne Hartwich; S. 17: Anne Hartwich; S. 19: Jesco Denzel/BPA; S. 20: Ed Gregory/pexels.com; S. 23: Bene Images/Shutterstock; S. 24: Bundesministerium des Innern; S. 25: BMI; S. 26: Fink & Fuchs Public Relations AG; S. 30: Leo Leowald/BSI (o.r.); S. 30: BSI; S. 31: BSI; S. 34: Fink & Fuchs Public Relations AG; S. 36: Bundesministerium für Verkehr und digitale Infrastruktur; S. 37: Ivan Smuk/Shutterstock; S. 38: Fink & Fuchs Public Relations AG; S. 40: Julia Tim/Shutterstock; S. 41: Anne Hartwich; S. 43: Matej Kastelic/Shutterstock; S. 44: Stephan Kohzer/BSI;

Das BSI-Magazin erscheint zweimal im Jahr. Es ist Teil der Öffentlichkeitsarbeit des BSI. Es wird kostenlos abgegeben und ist nicht zum Verkauf bestimmt.

Für die digitale Version des BSI-Magazins
scannen Sie den QR-Code

www.bsi.bund.de