BSI Forum

offizielles Organ des BSI
Bundesamt
für Sicherheit in der
Informationstechnik

Das IT-Sicherheitsgesetz – die neuen Aufgaben des BSI

Ziele des neuen IT-Sicherheitsgesetzes sind der Schutz der Bürger, die Verbesserung des IT-Sicherheitsniveaus insbesondere bei Kritischen Infrastrukturen sowie die Stärkung des Bundesamts für Sicherheit in der Informationstechnik (BSI). So müssen Betreiber Kritischer Infrastrukturen künftig ein Mindestniveau an IT-Sicherheit einhalten und erhebliche IT-Sicherheitsvorfälle an das BSI melden. Im Gegenzug ist das BSI verpflichtet, alle wesentlichen Informationen zur IT-Sicherheit zu sammeln und auszuwerten. Auf dieser Basis erhalten die Betreiber Kritischer Infrastrukturen zeitnah und umfassend alle relevanten Informationen über die IT-Sicherheitslage.

Interview mit Steve Ritter und Dr. Timo Hauschild, BSI

Nach langen Vorarbeiten und vielen Diskussionen ist das Gesetz zur Erhöhung der Sicherheit informationstechnischer Systeme (IT-Sicherheitsgesetz) im Juli 2015 in Kraft getreten (vgl. www.kritis.bund.de/SubSites/Kritis/DE/Rechtsrahmen/IT-SiG_node.html). Was ändert sich jetzt?

Steve Ritter (Referent „IT-Sicherheit und Recht“ im BSI): Mit dem IT-Sicherheitsgesetz ändert sich eine ganze Menge, sowohl für das BSI als auch für die Wirtschaft. Das BSI hat vom Gesetzgeber den klaren Auftrag erhalten, sich noch intensiver als bisher um die IT-Sicherheit der Bundesverwaltung zu kümmern. Es ist vorgesehen, dass das BSI vermehrt Mindeststandards erarbeitet, die alle Bundesbehörden umsetzen sollen beziehungsweise nach Verbindlicherklärung durch das Bundesministerium des Innern sogar umsetzen müssen.

Aber auch außerhalb der Bundesverwaltung soll das BSI künftig eine größere Rolle spielen. Am deutlichsten wird das im Bereich der Kritischen Infrastrukturen. Diese soll das BSI künftig unterstützen – entweder selbst oder durch qualifizierte Dienstleister – und noch stärker als schon heute mit Informationen versorgen. Dadurch sollen die Betreiber in die Lage versetzt werden, ihre IT besser abzusichern.

Nach dem Vorbild der zentralen Meldestelle für die Bundesverwaltung wird das BSI auch zur zentralen Meldestelle für IT-Sicherheit für Betreiber Kritischer Infrastrukturen.

Inhalt

Impressum

Redaktion:
Matthias Gärtner (verantwortlich)
E-Mail: matthias.gaertner@bsi.bund.de

Nora Basting
E-Mail: nora.basting@bsi.bund.de

Sebastian Bebel
E-Mail: sebastian.bebel@bsi.bund.de

Bundesamt für Sicherheit
in der Informationstechnik (BSI)
Referat Öffentlichkeitsarbeit und Presse
Postfach 20 03 63
53133 Bonn

Hausanschrift:
Godesberger Allee 185–189
53175 Bonn

Telefon: +49 228 999582-0
Telefax: +49 228 999582-5455

Web: www.bsi.bund.de
www.bsi-fuer-buerger.de

Das BSI-Forum, Organ des Bundesamtes für Sicherheit in der Informationstechnik in Bonn, ist Bestandteil der <kes> – Die Zeitschrift für Informations-Sicherheit
23. Jahrgang 2015

Verpflichtungen für Webseitenbetreiber und Hoster

Nach § 13 Absatz 7 TMG werden Diensteanbieter für geschäftsmäßig angebotene Telemedien zu einem besseren Schutz ihrer IT-Einrichtungen verpflichtet. Diensteanbieter sind je nach Fallgestaltung zum Beispiel die Betreiber einer Webseite und deren Webhoster. Soweit technisch möglich und wirtschaftlich zumutbar, müssen sie Maßnahmen nach dem Stand der Technik gegen unerlaubte Zugriffe auf ihre Systeme und personenbezogenen Daten sowie gegen Störungen (z. B. durch Angriffe) absichern. Eine der nach Beobachtungen des BSI am häufigsten unterlassenen Sicherungsmaßnahmen stellt beispielsweise das Nichteinspielen von Updates und Sicherheitspatches dar. Dadurch wird es Angreifern unter anderem erleichtert, über die jeweilige Webseite Schadsoftware an die Besucher der Webseite zu verteilen.

Wichtig: Unter die Regelung fallen nur gewerbliche Webseiten – private oder Vereinswebseiten werden also in der Regel nicht betroffen sein. Allerdings kann eine Webseite bereits dann gewerblich sein, wenn durch sie Einnahmen erzielt werden, etwa durch Werbung.

Diese sollen einerseits Informationen von der Meldestelle im BSI erhalten, aber andererseits auch eigene erhebliche IT-Sicherheitsvorfälle an das BSI melden, damit andere Betreiber rechtzeitig vor Angriffen gewarnt werden können.

Timo Hauschild (Referatsleiter „Schutz Kritischer Infrastrukturen“ im BSI): Was aber noch viel wichtiger ist: Betreiber Kritischer Infrastrukturen müssen ihre relevante IT künftig nach dem Stand der Technik absichern und die Umsetzung der Sicherheitsmaßnahmen durch regelmäßige Prüfungen belegen. Grund hierfür ist, dass heutzutage fast alle Sektoren der Kritischen Infrastrukturen, also zum Beispiel auch die Versorgung mit Wasser oder Lebensmitteln, von funktionierender IT abhängen. Daher müssen nicht mehr nur die Infrastrukturen selbst, sondern auch die dafür nötigen IT-Systeme abgesichert werden – zumindest wenn wir nicht eines Tages alle auf dem Trockenen sitzen wollen, weil ein Hacker sich Zugriff auf die IT eines Wasserwerks verschafft hat. Die Ausgestaltung der Absicherung bleibt größtenteils den Betreibern selbst überlassen. Lediglich für die Bereiche der Energienetze und -anlagen sowie der öffentlichen Telekommunikationsnetze werden konkrete Vorgaben durch die Bundesnetzagentur in Katalogen veröffentlicht – aufbauend auf Vorgaben, die es auch schon vor Inkrafttreten des IT-Sicherheitsgesetzes gab.

Verpflichtung der Provider

Betreiber öffentlicher Telekommunikationsnetze (das sind z. B. Telekommunikationsgesellschaften) und Anbieter von öffentlich zugänglichen Telekommunikationsdiensten (das sind z. B. E-Mail-Dienstanbieter) haben künftig beträchtliche Sicherheitsverletzungen an Netzen oder Diensten der Bundesnetzagentur (BNetzA) zu melden. Dazu gehören insbesondere auch solche Vorfälle, die zu unerlaubten Zugriffen auf die IT ihrer Kunden führen könnten.

Bei Bedarf kann die BNetzA die Öffentlichkeit informieren. Sofern die IT-Sicherheit betroffen ist, gibt die BNetzA die Informationen in jedem Fall an das BSI weiter. Die BNetzA kann die Netzbetreiber und Diensteanbieter zu Absicherungsmaßnahmen verpflichten. Wenn einem Diensteanbieter Störungen auf den IT-Systemen seiner Nutzer bekannt werden, ist er verpflichtet, diese Nutzer darüber zu informieren. Diese Pflicht besteht allerdings nur, sofern der Nutzer dem Anbieter bereits bekannt ist. Im zumutbaren Rahmen ist der Anbieter verpflichtet, seine Nutzer auf Werkzeuge (z. B. Antiviren-Programme) hinzuweisen, mit denen die Nutzer selbst diese Störungen erkennen und beseitigen können.

Was passiert jetzt gerade konkret?

Ritter: Die Melde- und Absicherungspflichten gelten nicht für alle zum gleichen Zeitpunkt. Schon jetzt müssen die Inhaber atomrechtlicher Genehmigungen IT-Sicherheitsvorfälle an das BSI melden. Auch die Betreiber öffentlicher Telekommunikationsnetze und -dienste müssen ihre verschärften Absicherungs- und Meldepflichten nach dem Telekommunikationsgesetz (TKG) sofort erfüllen. Eine Schonfrist haben hingegen die meisten Betreiber Kritischer Infrastrukturen. Denn erst in einer Rechtsverordnung wird endgültig festgelegt, was eine Kritische Infrastruktur – im Sinne des BSI-Gesetzes – ist. Daher können die entsprechenden Verpflichtungen vorher noch keine Wirkung entfalten.

Hauschild: Zurzeit arbeitet das Bundesministerium des Innern zusammen mit uns sowie den fachlich zuständigen Ministerien und Aufsichtsbehörden und auch mit Vertretern der Branchen an der Frage, welche Betreiber konkret unter die neuen Regelungen des BSI-Gesetzes fallen – das soll im Rahmen der BSI-KRITIS-Verordnung geregelt werden.

© BSI · 53133 Bonn · <kes> 2015#6

Die Verordnung wird in zwei Teilen erarbeitet: zuerst für die Sektoren Energie, IKT, Ernährung und Wasser, später dann für die Sektoren Transport und Verkehr, Finanzen und Gesundheit. Sobald die Verordnung in Kraft getreten ist, haben die betroffenen Betreiber zwei Jahre Zeit, um den Stand der Technik in Bezug auf ihre IT-Sicherheit umzusetzen und dem BSI nachzuweisen. Außerdem muss dem BSI eine Kontaktstelle benannt werden, über die die Meldungen an das BSI (und ggf. Rückfragen des BSI) erfolgen können. Dies muss spätestens sechs Monate nach Inkrafttreten der Verordnung passieren.

Das BSI bereitet sich aktuell intensiv auf die neuen Aufgaben vor. Hier gibt es noch viel zu tun. Beispielsweise müssen die Meldekriterien und Meldewege festgelegt werden. Außerdem muss konkretisiert werden, was „Stand der Technik" in Bezug auf IT-Sicherheit ist. Um hier Rechtssicherheit zu haben, können die Branchen branchenspezifische Sicherheitsstandards erarbeiten, die bei Eignung vom BSI anerkannt werden.

Wird das alles in der Rechtsverordnung geregelt?

Ritter: Diese Erwartung hört man häufig. Es ist aber so, dass sich die Regelungen einer Rechtsverordnung nur in dem Rahmen bewegen dürfen, der vom Gesetz vorgegeben ist. Im Fall des IT-Sicherheitsgesetzes darf das BMI in der Rechtsverordnung nur regeln, welche Einrichtungen, Anlagen oder Teile davon als Kritische Infrastrukturen im Sinne des BSI-Gesetzes anzusehen sind. Daher darf die Verordnung gar keine Regelungen zu Meldewegen, Meldeschwellen, Auditoren oder anderen Themen enthalten.

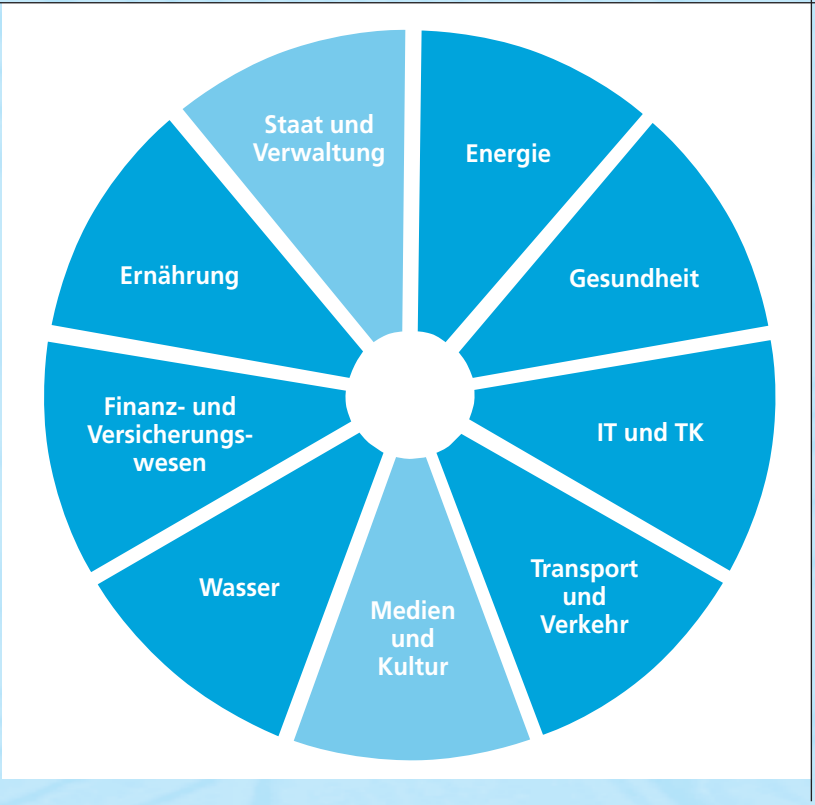
Hauschild: Genau, das IT-Sicherheitsgesetz ergänzt den seit Jahren mit dem UP KRITIS verfolgten kooperativen Ansatz zum Schutz Kritischer Infrastrukturen (www.upkritis.de, siehe auch <kes> 2013#4, S. 37) um einige wenige verpflichtende Elemente. Und ganz in diesem Sinne wird die Ausgestaltung des Gesetzes auch kooperativ angegangen. Schon heute sind wir in intensiven Diskussionen in den Gremien des UP KRITIS, um den Rahmen für die branchenspezifischen Sicherheitsstandards zu definieren. Gleiches gilt für die Umsetzung der Meldepflicht und die Bedarfe und Wünsche der Betreiber an die zukünftig durch das BSI zu verteilenden Informationen.

Die BSI-KRITIS-Verordnung hingegen regelt das „Wer?". Sie wird daher Angaben zu qualitativen und quantitativen Kriterien enthalten, anhand derer jeder KRITIS-Betreiber prüfen kann, ob er Anlagen betreibt, die zur Kritischen Infrastruktur im Sinne des Gesetzes gehören. Das qualitative Kriterium wird die Erbringung einer kritischen Dienstleistung sein: Eine solche Dienstleistung ist beispielsweise die Wasserversorgung, die Stromversorgung oder die Versorgung mit Lebensmitteln. Die quantitativen Kriterien enthalten hierzu dann Schwellenwerte, etwa in Bezug auf den Versorgungsgrad, denn letztlich geht es darum, wie viele Menschen von einer Anlage tatsächlich oder potenziell versorgt werden. Im Fokus stehen dabei immer die möglichen Folgen eines Ausfalls einer Anlage für die Bevölkerung in Deutschland.

Nun betreffen die Neuerungen durch das IT-Sicherheitsgesetz nicht ausschließlich die Betreiber Kritischer Infrastrukturen. Was ändert sich für die Bürger?

Ritter: Nun, von den Regelungen zum Schutz Kritischer Infrastrukturen profitieren die Bürger mittelbar. Sie bleiben dadurch hoffentlich von Ausfällen zum Beispiel des Stroms oder der Wasserversorgung verschont. Jedenfalls sollten solche dann nicht auf Hackerangriffe oder IT-Sicherheitsrisiken zurückgehen.

Aber es gibt auch eine Reihe von Regelungen, von denen die Bürger unmittelbar profitieren. So müssen zum Beispiel die Telekommunikationsanbieter ihre Nutzer



Die Kritischen Infrastrukturen sind in neun Sektoren unterteilt, von denen sieben von den Neuregelungen im IT-Sicherheitsgesetz betroffen sind.

Produktuntersuchungen durch das BSI

Um sichergehen zu können, dass ein IT-Produkt frei von Schwachstellen ist, sind eingehende Untersuchungen notwendig. Viele Untersuchungsmethoden des so genannten Reverse Engineering sind jedoch bisher mit rechtlichen Risiken behaftet. Damit das BSI seine Aufgaben im Hinblick auf die Bundesverwaltung und den Schutz Kritischer Infrastrukturen erfüllen kann, erhält es daher im neuen § 7a BSIG die Befugnis, IT-Produkte zu untersuchen. Stellt es bei seinen Untersuchungen Sicherheitslücken fest, darf es – nach vorheriger Einbindung des Herstellers – auch die Öffentlichkeit warnen, falls das erforderlich ist. Eine „Stiftung Warentest" für IT-Produkte wird das BSI dadurch jedoch nicht. Umfangreiche Tests und Vergleiche von IT-Produkten werden bereits heute in vielen Fachpublikationen veröffentlicht, mit denen das BSI nicht in Konkurrenz treten wird.

jetzt benachrichtigen, wenn sie feststellen, dass von deren IT-Systemen Störungen ausgehen – etwa weil sie Teil eines Botnetzes sind. Die Nutzer müssen außerdem auf Werkzeuge hingewiesen werden, mit denen sie diese Störungen erkennen und beseitigen können. Sie sind damit nicht mehr ganz auf sich allein gestellt, sondern können vom Wissen ihrer Telekommunikationsanbieter profitieren.

Eine der weitreichendsten Änderungen, von denen die Bürger profitieren werden, ist eine Änderung im Telemediengesetz (TMG), nämlich die Verpflichtung der Webseitenbetreiber und ihrer Hoster, ihre IT künftig nach dem Stand der Technik gegen unerlaubte Zugriffe und Störungen abzusichern. Dadurch soll es Angreifern erschwert werden, über seriöse Webseiten Schadsoftware zu verbreiten. Diese so genannten Drive-by-Downloads, bei denen sich die Nutzer durch den bloßen Besuch einer Webseite infizieren, sind nach wie vor ein großes Problem.

Doch auch der Diebstahl von personenbezogenen Daten der Bürger durch Angriffe auf Webserver wird durch die Umsetzung der Absicherungspflicht erschwert. Oftmals haben Webseitenbetreiber in der Vergangenheit selbst einfachste Maßnahmen, wie das Einspielen von Sicherheitspatches, unterlassen und den Angreifern den Datendiebstahl dadurch besonders leicht gemacht. Das ändert sich jetzt hoffentlich, sodass sich die Bürger sicherer im Internet bewegen können. ■

Verpflichtungen für KRITIS-Betreiber

Betreiber Kritischer Infrastrukturen werden durch die Neuregelungen des BSI-Gesetzes dazu verpflichtet, ihre informationstechnischen Systeme, Komponenten und Prozesse, die für die Funktionsfähigkeit der von ihnen betriebenen Kritischen Infrastrukturen maßgeblich sind, gemäß dem Stand der Technik abzusichern, um Störungen oder Ausfälle dieser Systeme zu vermeiden.

Die Betreiber müssen regelmäßig – spätestens alle zwei Jahre – die Einhaltung des Stands der Technik gegenüber dem BSI nachweisen. Der Stand der Technik kann für eine Branche im Rahmen eines branchenspezifischen Sicherheitsstandards konkretisiert werden, den die jeweiligen Branchen erarbeiten können. Außerdem werden die unter das Gesetz fallenden KRITIS-Betreiber verpflichtet, erhebliche Sicherheitsvorfälle, das heißt Störungen der Verfügbarkeit, Integrität, Authentizität und Vertraulichkeit, welche die Funktionsfähigkeit der Kritischen Infrastrukturen beeinträchtigen können oder beeinträchtigt haben, an das BSI zu melden.

Das BSI wird zudem zur zentralen Meldestelle für Betreiber Kritischer Infrastrukturen in Bezug auf die Sicherheit in der Informationstechnik. Es bekommt die Aufgabe, Informationen, die für die Abwehr von Gefahren für die Informationstechnik wesentlich sind, zu sammeln, auszuwerten und deren potenzielle Auswirkungen auf die Verfügbarkeit der Kritischen Infrastrukturen zu untersuchen, ein Lagebild zu erstellen und kontinuierlich fortzuschreiben und die KRITIS-Betreiber sowie die zuständigen (Aufsichts-)Behörden zu unterrichten. KRITIS-Betreiber werden durch das Gesetz also nicht nur zur Meldung verpflichtet, sondern erhalten im Gegenzug vom BSI Informationen, Bewertungen und Empfehlungen.

Darüber hinaus kann das BSI die KRITIS-Betreiber auf deren Wunsch bei der Sicherung ihrer Informationstechnik beraten und unterstützen oder auf qualifizierte Sicherheitsdienstleister verweisen. Damit wird die Zuständigkeit des BSI für die Sicherheit der Informationstechnik der Bundesverwaltung erweitert auf die Kritischen Infrastrukturen. (www.kritis.bund.de/SubSites/Kritis/DE/Rechtsrahmen/IT-SiG_node.html).

© BSI · 53133 Bonn · <kes> 2015#6

De-Mail in der digitalen Verwaltung

Wo stehen wir? Wie geht es weiter?

Der elektronische Schriftverkehr ist längst integraler Bestandteil der Kommunikationsprozesse in der Verwaltung. Unter sicherheitstechnischen Gesichtspunkten – insbesondere in Bezug auf ihre Vertraulichkeit, Integrität und Authentizität – besitzt die E-Mail jedoch noch Entwicklungspotenzial. Hier greift das Konzept von De-Mail, das speziell auf diese Bedürfnisse nach Sicherheit und Zuverlässigkeit abgestimmt ist.

Von Ingrid Grüning, BSI

De-Mail basiert architektonisch auf einem geschlossenen Kommunikationsverbund, in dem ausschließlich vom Bundesamt für Sicherheit in der Informationstechnik (BSI) akkreditierte De-Mail-Diensteanbieter zugelassen sind, die zuvor einen umfangreichen Prüfprozess erfolgreich abgeschlossen haben. Die entsprechenden Anforderungen sind insbesondere in den „Technischen Richtlinien De-Mail" des BSI (TR-01201) festgelegt.

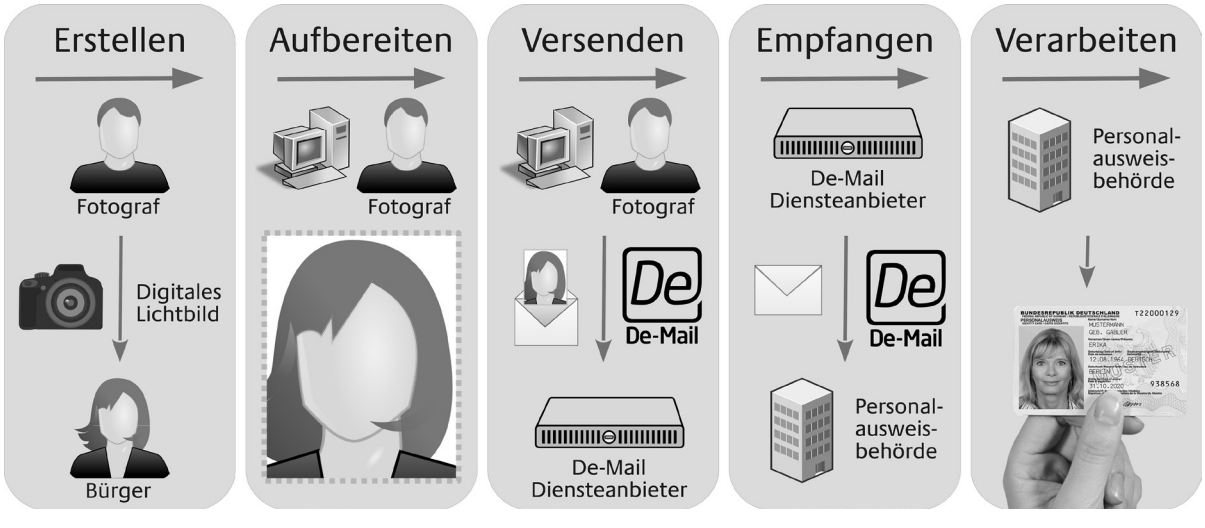
Nicht zuletzt durch den Einsatz von verschlüsselten Versandkanälen und der zuverlässigen Identifizierung aller Kommunikationspartner innerhalb des De-Mail-Verbundes ermöglicht De-Mail den vertraulichen und verbindlichen Versand von Dokumenten und Nachrichten.

Dennoch: De-Mail hat nicht den Anspruch, die herkömmliche E-Mail zu ersetzen. Es eröffnet vielmehr für ausgewählte Einsatzzwecke Möglichkeiten, die klassischen Vorteile der E-Mail als schnelles und unkompliziertes Medium mit einem hohen Anspruch an Sicherheit, Vertraulichkeit und Unverfälschbarkeit zu verbinden.

Die Entwicklung von De-Mail

Die Grundsteinlegung für De-Mail erfolgte im Mai 2011 mit Inkrafttreten des „Gesetzes zur Regelung von De-Mail-Diensten und zur Änderung weiterer Vorschriften" (De-Mail-Gesetz). 2012 und 2013 ließen sich insgesamt vier De-Mail-Diensteanbieter durch das BSI akkreditieren und etablierten diesen Dienst deutschlandweit am Markt. Akkreditierte De-Mail-Diensteanbieter sind derzeit: 1&1 de-Mail GmbH, Mentana-Claimsoft GmbH, Telekom Deutschland GmbH und T-Systems International GmbH.

Seit dem E-Government-Gesetz des Bundes (EGovG) von 2013 kann die Schriftform unter bestimmten Bedingungen auch durch eine De-Mail erfüllt werden (§ 3a Absatz 2 Satz 4 Nr. 2 VwVfG). Hiermit wird die Breite der Anwendungsmöglichkeiten von De-Mail gerade im Bereich der Kommunikation zwischen Bürgern und Behörden deutlich erweitert. Nach § 2 EGovG ist ab März 2016 jede Bundesbehörde verpflichtet, einen Zugang für eine Übermittlung elektronischer Dokumente über De-Mail anzubieten.



Elektronische Bildübermittlung an Ausweisbehörden per De-Mail

Die zentrale Infrastruktur für eine Anbindung an den De-Mail-Verbund wird den Bundesbehörden seit März 2015 vom Bund zur Verfügung gestellt. Mithilfe dieses so genannten Bundesgateways ist es den Bundesbehörden in einem vereinfachten Verfahren möglich, ihre Behördeneigene E-Mail-Infrastruktur an den De-Mail-Verbund anzuschließen. Das Versenden und Empfangen von De-Mails kann somit in der Regel direkt vom gewohnten E-Mail-Client an den Arbeitsplätzen der Mitarbeiter erfolgen. Die beschriebene Anbindung seitens der Bundesbehörden erfolgt nun sukzessive bis zum März 2016.

Somit steht sowohl Bürgern als auch Wirtschaft fortan mindestens eine Adresse der jeweiligen Behörde zur Verfügung, an die De-Mails gesendet werden können. Das Einsparpotenzial liegt auf der Hand: Hierdurch lassen sich im Vergleich zum klassischen Postweg Sendevorgänge beschleunigen beziehungsweise Behördengänge vermeiden.

Um die Vorteile und das Potenzial von De-Mail auch behördenseitig voll auszuschöpfen, ist eine weitaus tiefere Integration von De-Mail auch in interne Verwaltungs- und weitere externe Kommunikationsprozesse seitens der Behörde möglich. Diese kann beispielsweise über eine zusätzliche Einbindung von De-Mail in vorhandene Fachverfahren und Dokumentenmanagementsysteme umgesetzt werden, sodass etwa eingesandte Dokumente medienbruchfrei intern weiterverarbeitet und nach Abschluss des Vorgangs elektronisch archiviert werden können.

Erfahrungen mit der Integration

Erste Erfahrungen mit der Integration von De-Mail in ein Fachverfahren konnten die Städte Köln und Göttingen im Rahmen des 2014 durchgeführten Pilotprojektes „Elektronische Bildübermittlung“ sammeln.

In diesem Projekt wurden, auf Wunsch und mit der Zustimmung des jeweiligen Antragsstellers, die für die Ausstellung eines neuen Personalausweises benötigten biometrischen Passbilder von teilnehmenden Fotografen nach der Aufnahme auf direktem Wege sicher und vertraulich per De-Mail zur Personalausweisbehörde gesendet.

Der zuvor nötige Prozess des Entwickelns beziehungsweise Ausdruckens des Lichtbilds als Foto und des späteren Wiedereinscannens in der Behörde konnte somit komplett entfallen.

Die in diesem Pilotprojekt gewonnenen Erfahrungswerte sind nach erfolgreichem Abschluss des Projekts in die vom BSI entwickelte technische Richtlinie BSI TR-03146 „Elektronische Bildübermittlung zur Beantragung hoheitlicher Dokumente (E-Bild hD)“ eingeflossen, die seit dem 1. November 2014 zur Verfügung steht. In dieser technischen Richtlinie werden die organisatorischen Anforderungen an das gesamte Verfahren und insbesondere auch die Anforderungen an den De-Mail-Versand spezifiziert. Nach Abschluss der Pilotierungsphase wurde das Verfahren in den teilnehmenden Städten in den Wirkbetrieb überführt. ■

Amtliche Mitteilungen

1. Im Vergleich zur letzten Ausgabe dieser amtlichen Mitteilungen sind inzwischen folgende Zertifizierungen des BSI gemäß Common Criteria und ITSEC abgeschlossen worden:

Hersteller/Vertreiber	Produkt	Produkt-Typ	Ergebnis ID Zertifizierungsdatum
MaskTech International GmbH	MTCOS Pro 2.2 EAC with PACE / P60D080PVC - V2 (BAC)	Smartcard mit Passanwendung (BAC)	BSI-DSZ-CC-0893-2014-MA-01 2015-08-31
Stoneridge Electronics AB	Digital Tachograph (Vehicle Unit) SE5000, Version 7.6	Fahrtenschreiber	E3/hoch BSI-DSZ-ITS EC-0959-2015 2015-08-18
Giesecke & Devrient GmbH	STARCOS 3.6 COS C1	Smartcard mit Anwendung (eHealth)	EAL 4+ BSI-DSZ-CC-0916-2015 2015-08-07

© BSI · 53133 Bonn · <kes> 2015#6

Hersteller/Vertreiber	Produkt	Produkt-Typ	Ergebnis ID Zertifizierungsdatum
Continental Automotive GmbH	Digital Tachograph DTCO 1381, Release 2.2a	Fahrtenschreiber	BSI-DSZ-CC-0936-2015-MA-01 2015-08-05
Infineon Technologies AG	Infineon smart card IC (Security Controller) M7820 A11 with optional RSA2048/4096 v1.02.013, EC v1.02.013, SHA-2 v1.01 and Toolbox v1.02.013 libraries and with specific IC dedicated software	Smartcard Controller	EAL 5+ BSI-DSZ-CC-0829-V2-2015 2015-08-03
T-Systems International GmbH	TCOS FlexCert 2.0, Release 1/ SLE78CLX1440P	Smartcard mit Anwendung (eHealth)	EAL 4+ BSI-DSZ-CC-0904-2015 2015-07-03
Infineon Technologies AG	Infineon Technologies Security Controller M7794 A12 and G12 with optional RSA2048/4096 v1.02.013 or v2.00.002, EC v1.02.013 or v2.00.002 and Toolbox v1.02.013 or v2.00.002 libraries and with specific IC-dedicated software	Smartcard Controller	EAL 5+ BSI-DSZ-CC-0964-2015 2015-06-12

Anmerkung:
- Die zugehörigen Zertifizierungsreporte mit Zertifikaten sind auf der Web-Seite www.bsi.bund.de/zertifizierungsreporte einzusehen.

2. Im Vergleich zur letzten Ausgabe dieser amtlichen Mitteilungen ist inzwischen für folgende Produkte eine Zertifizierung beantragt worden:

Antragsteller	Produktname	Produkttyp	Zertifizierungs-ID
Red Hat Tower	Red Hat Enterprise Linux Version 7.1	Betriebssystem	BSI-DSZ-CC-0999
OpenLiMiT SignCubes AG	SecDocs Security Komponenten, Version 2.4	Middleware	BSI-DSZ-CC-0994

Anmerkungen:
- Eine Veröffentlichung dieser Angaben erfolgt hier nur, sofern der Antragsteller damit einverstanden ist *und* die Evaluierung begonnen wurde. In der Liste vorhandene Nummerierungslücken betreffen beantragte Zertifizierungen, für die die genannten Voraussetzungen fehlen.
- Bei einigen Produkten handelt es sich um eine Re-Zertifizierung eines bereits zertifizierten Produktes wegen Änderungen am Produkt oder Wechsel der Prüfkriterien.

3. Vom BSI zertifizierte und registrierte Schutzprofile

Entwickler	Profilbezeichnung Zertifizierungsdatum	ID
Bundesamt für Sicherheit in der Informationstechnik	Common Criteria Protection Profile Electronic Health Card Terminal (eHCT), Version 3.6	EAL 3+ BSI-CC-PP-0032-V2-2015 2015-09-17

4. Vom BSI erteilte Standortzertifikate

Antragsteller	Entwicklungs-/ Produktionsstandorte	ID Ausstellungsdatum	gültig bis
NXP Semiconductors Austria GmbH (NXP)	NXP Semiconductors Austria GmbH, Mikron-Weg 1, 8101 Gratkorn, Austria, Business Unit Identification (BU ID)	BSI-DSZ-CC-S-0042-2015 2015-08-17	2017-08-16
NedCard BV	Standort Wijchen: Bijsterhuizen 25-29, NL-6604LM Wijchen, Netherlands	BSI-DSZ-CC-S-0043-2015 2015-08-14	2017-08-13

5. Vom BSI erteilte ISO-27001-Zertifikate auf der Basis von IT-Grundschutz

Zertifikatsnummer	Institution	Untersuchungsgegenstand	gültig bis
BSI-IGZ-0185-2015	Bechtle – Systemhaus GmbH & Co.KG	Untersuchungsgegenstand ist das Installationszentrum des Bechtle IT-Systemhauses Ober-Mörlen für Anwender-spezifische Software-Installationen. In einem ersten Schritt wurde beispielhaft für das Projekt „HessenPC“ für das Land Hessen eine sichere Installationsumgebung aufgebaut und überprüft. Beschrieben und zertifiziert wurde damit einhergehend die sichere Massenbetankung von Kunden-Clients (PC-Systeme, ThinClients oder Notebooks) mit Betriebssystem- und Anwender-spezifischer Client-Software, sowie alle damit zusammenhängenden relevanten Prozesse.	2018-07-19
BSI-IGZ-0213-2015	Informationsverbund der ekom21 – KGRZ Hessen	Der Untersuchungsgegenstand umfasst die informationstechnischen Anlagen und Lösungen der ekom21 KGRZ Hessen an den Standorten Darmstadt, Gießen und Kassel, die zur Erbringung der ASP -Dienstleistungen erforderlich sind. Betrachtet wird die IT-Infrastruktur, die zur Erfüllung der Aufgaben an den genannten Standorten dient. Nicht Gegenstand der Untersuchung sind ASP-Dienste die auslaufenden Charakter haben und deshalb für die Restlaufzeit outgesourct wurden.	2018-07-07

© BSI · 53133 Bonn · <kes> 2015#6