BSI Forum

offizielles Organ des BSI
Bundesamt
für Sicherheit in der
Informationstechnik

Messepräsenz

CeBIT 2016

Vom 14. bis zum 18. März 2016 präsentiert sich das Bundesamt für Sicherheit in der Informationstechnik (BSI) auf der CeBIT in Hannover.

Auf der Messe informieren Mitarbeiterinnen und Mitarbeiter des BSI zu den Themen:

_____ Cloud-Computing

_____ IT-Sicherheitsgesetz

_____ Allianz für Cyber-Sicherheit

_____ sicheres mobiles Arbeiten

_____ Sicherheitsberatung

_____ IT-Grundschutz

_____ IT-Sicherheitszertifizierung

_____ BSI für Bürger

_____ Jobs@BSI

Unter www.bsi.bund.de/Veranstaltungen finden Sie ausführliche Informationen zu den genannten Messethemen.

Darüber hinaus tragen BSI-Experten im Convention Center (CC), Saal 104, zu folgenden Themen vor:

Mittwoch, 16. März 2016
11.00–13.00 Uhr
Cloud-Computing – Neuer Anforderungskatalog des BSI und Cloud-Security-Label

Mittwoch, 16. März 2016
13.00–15.00 Uhr
Modernisierung des IT-Grundschutzes

Der Messestand des BSI befindet sich in Halle 6, Stand G 29. ■

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
24. Jahrgang 2016

Zahlungsverkehr und öffentliche Hand

Was ist bei der Umsetzung von § 4 EGovG zu beachten?

Mit dem E-Government-Gesetz (EGovG) hat der deutsche Gesetzgeber 2013 die Digitalisierung der öffentlichen Verwaltung eingeleitet. Fallen im Rahmen eines elektronisch durchgeführten Verwaltungsverfahrens Gebühren oder sonstige Forderungen an, muss die Behörde die Begleichung dieser Forderungen durch Teilnahme an mindestens einem im elektronischen Geschäftsverkehr üblichen und hinreichend sicheren Zahlungsverfahren ermöglichen, § 4 EGovG. Was ist bei der Umsetzung von § 4 EGovG aus Sicht der Behörde zu beachten?

Von Dr. Josef Kokert, Bundesanstalt für Finanzdienstleistungsaufsicht (BaFin)

Zunächst einmal ist die Frage zu klären, welche Rolle eine Behörde bei der Teilnahme an einem elektronischen Zahlungsverfahren einnimmt: Ist die Behörde ein Zahlungsdienstleister oder ein Zahlungsdienstnutzer? Diese grundsätzliche Unterscheidung treffen § 675 f Abs. 3 Bürgerliches Gesetzbuch (BGB) und § 1 Zahlungsdiensteaufsichtsgesetz (ZAG). Von dieser Unterscheidung hängen zahlreiche Pflichten ab, wie zum Beispiel eine Erlaubnispflicht nach dem ZAG.

Im Kontext des § 4 EGovG soll der Bürger (Zahler) Buchgeld (Zahlungsmittel) auf ein Konto der Behörde (Zahlungsempfänger) übermitteln. Diese Buchgeldübermittlung wird Zahlungsvorgang genannt. Zur Ausführung des Zahlungsvorgangs beauftragt der Bürger seinen Zahlungsdienstleister. Der Auftrag kann unmittelbar oder mittelbar über die Behörde erteilt werden. Folglich ist die Behörde bei der Teilnahme an einem elektronischen Zahlungsverfahren als Zahlungsempfänger lediglich ein Zahlungsdienstnutzer. Die Behörde wird insbesondere durch die Übermittlung des Zahlungsauftrags an den Zahlungsdienstleister nicht selbst zum Zahlungsdienstleister.

Ermöglichung eines elektronischen Zahlungsverfahrens

Wie ermöglicht die Behörde dem Bürger die Teilnahme an einem elektronischen Zahlungsverfahren? Dazu benötigen beide Parteien mindestens einen Zahlungsdienstleister, der den Zahlungsvorgang von dem Konto des Zahlers auf das Konto des Zahlungsempfängers ausführt. Nach dem ZAG dürfen nur lizenzierte Zahlungsdienstleister Zahlungskonten führen. Der Zahlungsdienstleister wird als Zahlungsgeschäft die Lastschrift, die Überweisung oder die Kartenzahlung anbieten, § 1 Abs. 2 Nr. 2 ZAG.

Beispiel: Hat eine Behörde einem Bürger schriftlich eine gebührenpflichtige Erlaubnis erteilt, so wird der Bürger beispielsweise seinen Zahlungsdienstleister – in der Regel eine Bank – beauftragen, einen Geldbetrag von seinem Konto auf das Konto der Behörde zu überweisen, das bei einem anderen Zahlungsdienstleister geführt wird. War früher ein ausgefülltes Überweisungsformular (beleggebunden) der übliche Weg der Auftragserteilung, so kommen in der digitalen Welt neue elektronische Verfahren (beleglos) zum Einsatz – weit verbreitet ist das Online-Banking: Der Bürger wählt sich über das Internet in sein Konto ein und erteilt seiner Bank

Das E-Government-Gesetz (EGovG) formuliert für Bundesbehörden die Rahmenbedingungen zur Mitwirkung an der Digitalen Agenda. Bund, Länder und Kommunen sollen in Zukunft für die Umsetzung von Bundesrecht einfachere, nutzerfreundlichere und effizientere elektronische Verwaltungsdienste anbieten. Die im § 4 EGovG formulierte Anforderung zur Bereitstellung elektronischer Zahlverfahren wirft Fragen zu deren Umsetzung auf. Die folgenden drei Artikel sind Ergebnis einer fachlichen Kooperation der Bundesanstalt für Finanzdienstleistungsaufsicht (BaFin) und des BSI über elektronische Zahlungsdienste gemäß § 4 EGovG und verstehen sich als Hilfestellung zur Umsetzung dieser Vorschrift.

Der Artikel „Zahlungsverkehr und öffentliche Hand – Was gilt es zu beachten?“ nimmt eine juristische Bewertung der sich aus § 4 EGovG für Behörden ergebenden Umsetzungspflichten vor. Die technischen Mindestanforderungen an elektronische Zahlungsdienste der Finanzaufsicht BaFin beschreibt der Artikel „Technische Auswirkungen der Zahlungsdiensteregulierung auf Online-Angebote von Behörden“. Abschließend betrachtet der Artikel „Elektronische Zahlungsdienste – Sicher! Aber wie?“ die Beschaffungsanforderungen aus Sicht des Informationssicherheitsmanagements.

unmittelbar elektronisch den Zahlungsauftrag.

Die Behörde erfüllt in diesem einfachen Beispiel ihre Pflicht aus § 4 EGovG, wenn sie in der elektronischen Erlaubniserteilung eine „Internationale Bankkontonummer" (IBAN) angibt, auf das die Gebühr zu zahlen ist. Die Überweisung per Online-Banking stellt also ein weit verbreitetes elektronisches Zahlungsverfahren dar, unabhängig davon, ob die Zahlung vom heimischen PC, vom Smartphone oder über die Spracherkennung telefonisch ausgelöst wird.

Die Intention von § 4 EGovG geht jedoch weiter: Die Behörde soll geeignete Verwaltungsangelegenheiten über das Internet möglichst abschließend ohne Medienbrüche erledigen. Die Idealvorstellung ist, die Anliegen der Bürger elektronisch entgegenzunehmen, zu bearbeiten, zu bescheiden und auch zahlungstechnisch beleglos abzuwickeln. Der Bürger soll das Verwaltungsgebäude nicht aufsuchen müssen.

Deshalb gilt es, dem Bürger die elektronische Erfüllung seiner Zahlungsverpflichtung mit wenigen Klicks zu ermöglichen und zugleich aufseiten der Verwaltung die automatisierte Einlieferung der Sollstellung, die Überwachung des Zahlungseingangs und die Verbuchung auszulösen. Die Ermöglichung eines elektronischen Zahlungsverfahrens bedeutet im Ergebnis für die Behörde, dass auf der Serviceplattform eine Schnittstelle eines Zahlungsdienstleisters integriert wird, die dem Bürger eine Zahlung ermöglicht.

Übliche Zahlungsverfahren

Bei der Frage, welchen Zahlungsdienstleister die Behörde auf ihrer Serviceplattform integrieren soll, lenkt § 4 EGovG den Blick zunächst auf die Üblichkeit des Zahlungsverfahrens. Übliche Zahlungsverfahren sind beispielsweise SEPA-Überweisungen, SEPA-Lastschriften, Kartenzahlungen und E-Payment-Verfahren.

Die Akzeptanz dieser Zahlungsverfahren kann sich rasch ändern, etwa weil sich die gesetzlichen Rahmenbedingungen ändern, sich neue und anwenderfreundliche Innovationen durchsetzen oder Sicherheitsprobleme auftauchen, die von einem Zahlungsdienstleister nicht beseitigt werden können. Die Behörde sollte deshalb zur Erfüllung der Anforderung „Üblichkeit" lediglich darauf achten, dass das angebotene Zahlungsverfahren anwenderfreundlich ist und den spezifischen Anforderungen der Behörde entspricht.

Sichere Zahlungsverfahren

Zentrales Auswahlkriterium für das Zahlungsverfahren ist vielmehr gemäß § 4 EGovG das Kriterium der Sicherheit im Sinne der Informationssicherheit. Die Behörde darf also nicht ungeprüft irgendein auf dem Markt angebotenes elektronisches Zahlungsverfahren auswählen – die Behörde muss nach eingehender Prüfung zu dem Ergebnis kommen, dass dieses Zahlungsverfahren auch hinreichend sicher ist.

Dass diese Sicherheitsprüfung unerlässlich ist, ergibt sich darüber hinaus auch aus der Stellung der Behörde. Behörden selbst sind verpflichtet, für die Durchführung des elektronischen Verwaltungsverfahrens die Informationssicherheit zu gewährleisten, siehe § 10 EGovG. Zum Verwaltungsverfahren gehört auch das Zahlungsverfahren, sobald es seitens der Behörde über eine Serviceplattform angeboten wird.

Schließlich ergibt sich die Notwendigkeit der Informationssicherheit bei Zahlungsverfahren auch aus einem rein praktischen Grund: Jahr für Jahr wächst die Bedrohung durch Cyberkriminalität und diese hat insbesondere den Zahlungsverkehr im Fokus. Kann die Informationssicherheit der dem Bürger zur Verfügung gestellten Serviceplattform und des dort integrierten Zahlungsverfahrens dem Angriffsniveau der Kriminellen nicht standhalten, sind – abgesehen vom Reputationsverlust der Behörde – Haftungsfragen und Kosten zur Wiederherstellung der Informationssicherheit absehbar.

Lizenzierte Zahlungsdienstleister

Eine erste Hilfestellung für die Prüfung der Behörde, ob das ausgewählte Zahlungsverfahren sicher ist, kann der Rückgriff auf einen lizenzierten Zahlungsdienstleister sein. Gewöhnlich veröffentlichen die nationalen Aufseher in Europa auf ihrer Homepage eine Liste der lizenzierten Zahlungsdienstleister. In Deutschland benötigen Zahlungsdienstleister im Sinne des § 1 Abs. 1 Nr. 1 oder Nr. 5 ZAG entweder eine Erlaubnis nach § 32 KWG oder nach § 8 ZAG. Welches Unternehmen eine entsprechende Erlaubnis besitzt, kann auf der Homepage der BaFin unter „Daten & Dokumente/Alle Datenbanken" eingesehen werden.

Ein beaufsichtigtes Unternehmen muss über eine ordnungsgemäße Geschäftsorganisation verfügen, die auch eine ordnungsgemäße IT-Organisation umfasst. Zu Letzterer gehört unter anderem ein Informationssicherheitsmanagement. Zudem müssen Zahlungsdienstleister die Mindestanforderungen an die Sicherheit von Internetzahlungen erfüllen, die in dem Rundschreiben 4/2015 der BaFin vom 5. Mai 2015 aufgenommen wurden. Dazu gehört, dass Zahlungsdienstleister ein allgemeines Sicherheits- und Kontrollumfeld einrichten sowie spezifische Sicherheits- und Kontrollmaßnahmen bei Internetzahlungen durchführen. Zudem ist der Zahlungsdienstleister zur

Kundenaufklärung, -information und -kommunikation verpflichtet.

Ein Zahlungsverfahren kann somit nur dann in diesem Kontext als hinreichend sicher angesehen werden, wenn die Anforderungen des Rundschreibens 4/2015 eingehalten werden. Insoweit sollte die von einem lizenzierten Zahlungsdienstleister angebotene Software zur Implementierung des Zahlungsverfahrens grundsätzlich allen Anforderungen der Informationssicherheit genügen. Die Behörde wird indes versuchen, das Zahlungsverfahren mit den verschiedenen behördeninternen Fachverfahren zu verknüpfen und einen Datenaustausch zu ermöglichen. Zum Beispiel können aus dem Fachverfahren der Name des Bürgers, das Aktenzeichen, das Kassenzeichen, die empfangsberechtigte Kasse mit IBAN und gegebenenfalls BIC in das Zahlungsverfahren überführt werden, um eine SEPA-Überweisung vorzubereiten.

Bietet des Weiteren der Zahlungsdienstleister eine Information über die erfolgreiche Durchführung einer Zahlung an die Behörde an, so kann diese Information dazu genutzt werden, um in der Behörde die Verbuchung auszulösen. Wird eine derart aufeinander abgestimmte Lösung angestrebt, so hat die Behörde zusätzlich zu prüfen, ob diese Lösung auch ihren Sicherheitsanforderungen entspricht.

Mit der Annahme der überarbeiteten Zahlungsdiensterichtlinie am 8. Oktober 2015 durch das europäische Parlament wurden die Voraussetzungen für die aufsichtsrechtliche Zulassung so genannter Dritter Zahlungsdienstleister geschaffen. Zukünftig werden unter anderem Zahlungsdienstleister beaufsichtigt, die Zahlungen auf Konten auslösen, ohne diese Konten selbst zu führen. Diese Zahlungsdienste richten eine Softwarebrücke zwischen der Website eines Händlers und der Plattform des kontoführenden Zahlungsdienstleisters des Zahlers ein, um auf Überweisungen gestützte Zahlungen über das Internet auszulösen.

Die Zahlungsdiensterichtlinie bedarf noch eines nationalen Umsetzungsgesetzes. Die Europäische Bankenaufsichtsbehörde (EBA) erarbeitet derzeit weitere konkretisierende Anforderungen für die Frage, wie eine sichere Kommunikation zwischen den Zahlungsauslösediensten und den kontoführenden Zahlungsdienstleistern erfolgen soll. Auch werden die Anforderungen an die so genannte starke Authentifizierung der Kunden, die vor einer Zahlung durchgeführt werden muss, konkretisiert. Diese Konkretisierungen werden als so genannte „Regulatory Technical Standards“ für alle Zahlungsdienstleister direkt verbindlich werden. Die durch die Zahlungsdiensterichtlinie eingeleitete Marktöffnung verbreitert für Behörden die Auswahlmöglichkeiten für die Zahlungsverfahren.

Bereits heute werden in Europa Zahlungsauslösedienste angeboten. Ob diese Zahlungsdienste als hinreichend sicher beurteilt werden können, kann derzeit mangels konkreter aufsichtsrechtlicher Anforderungen nicht beurteilt werden. Hier bietet sich für Behörden der Rückgriff auf die allgemeinen Anforderungen an die Informationssicherheit sowie auf die Mindestanforderungen an die Sicherheit von Internetzahlungen an. Behörden könnten von den so genannten „Dritten Zahlungsdienstleistern“ den Nachweis einfordern, dass das angebotene Zahlungsverfahren die allgemeinen Anforderungen an die Informationssicherheit und die Mindestanforderungen an die Sicherheit von Internetzahlungen einhält. Zusätzlich wird die Beachtung des Sicherheitsniveaus der Behörde zu prüfen sein, wenn die von einem „Dritten Zahlungsdienstleister“ angebotene Softwarebrücke in die Fachanwendungen der Behörde eingebunden wird.

Nutzung von IT-Dienstleistern

In der Praxis werden Behörden ihre Serviceplattform häufig nicht selbst betreiben, sondern durch einen IT-Dienstleister betreiben lassen; auch Zahlungsdienstleister bedienen sich häufig eines oder mehrerer IT-Dienstleister.

Durch den Rückgriff auf IT-Dienstleister entfällt nicht die Verantwortung der Behörde gemäß § 4 EGovG, dem Bürger ein hinreichend sicheres Zahlungsverfahren anzubieten. Die Behörde wird dafür Sorge tragen, dass sowohl der von ihr beauftragte IT-Dienstleister als auch der Zahlungsdienstleister und dessen IT-Dienstleister die Anforderungen an die Informationssicherheit sowie die besonderen Anforderungen an die Sicherheit von Internetzahlungen aus dem Rundschreiben 4/2015 der BaFin einhalten – dies ist ein dauerhafter Prozess. Behörden sollten deshalb eine IT-Dienstleistersteuerung sowie eine Steuerung des Zahlungsdienstleisters auf der Grundlage von Berichts- und Nachweispflichten einrichten. ■

Technische Auswirkungen der Zahlungsdiensteregulierung auf Online-Angebote von Behörden

In zunehmendem Maße bieten Behörden den Bürgern Dienstleistungen online an. Soweit hierbei Gebühren anfallen, wird hier – beispielsweise zur Freigabe eines kostenpflichtigen Downloads – teilweise eine sofortige Bestätigung der Zahlungsausführung gewünscht sein. Wie wirken die aktuelle und kommende Regulierung von Zahlungsdienstleistern Risiken bei der Nutzung dieser Dienste durch Behörden entgegen?

Von Dr. Markus Held, BSI

Durch das Angebot von Online-Diensten entstehen Risiken für die Vertraulichkeit, Integrität und Authentizität von Daten. Aufgrund der hohen öffentlichen Sichtbarkeit des Online-Angebots ergeben sich zusätzlich Reputationsrisiken. Rechtsrisiken können sich aus der Komplexität der Zahlungsdiensteregulierung und Einzelfallentscheidungen des Zahlungsverkehrsrechts ergeben. Im Folgenden konzentrieren wir uns auf die Risiken, die sich im Online-Zahlungsverkehr eines Behörden-Webangebots ergeben.

Nutzbarkeit der unterstützten Zahlungsdienste

Keine Behörde wird in der Praxis alle am Markt verfügbaren Zahlungsdienste in ihrem Angebot unterstützen können. Gleichzeitig wird jeder einzelne Bürger selbst nur für bestimmte Zahlungsdienste bereit sein, diese zu nutzen. Es besteht somit das Risiko, dass einzelne Bürger nicht dazu in der Lage sein werden, eine der angebotenen Zahlungsarten zu nutzen. Verschärft wird diese Problematik durch die Frage, ob es überhaupt zumutbar ist, die Nutzung eines bestimmten Zahlungsdienstes fest vorzusehen.

Ausfall des Zahlungsdienstes

Online-Zahlungsdienste können aus verschiedenen Gründen ausfallen: Dies kann sich zeitweise beispielsweise durch Softwarefehler, Fehlkonfigurationen oder Hardware-Schäden aufseiten des Zahlungsdienstleisters ergeben. Ein dauerhafter Ausfall kann sich auch durch die Insolvenz des Zahlungsdienstleisters ergeben.

Datendiebstahl

Bürger und Behörden haben ein Interesse an der Vertraulichkeit ihrer Zahlungsdaten. Dies gilt in besonderem Maße für Authentifizierungsdaten (z. B. PIN/TAN) und für personenbezogene Daten in Zahlungsformularen. Auch die Transaktionsdaten (Überweisungsbeträge, Ziel- und Quellkonten) werden vertraulich zu behandeln sein, allein schon weil sie (in Summe) Rückschlüsse auf die wirtschaftliche Situation von Zahler oder Zahlungsempfänger erlauben können.

Der Diebstahl von Zahlungsdaten kann Betrug ermöglichen oder zumindest erleichtern. Betrug im Online-Zahlungsverkehr zeigt sich vor allem dann, wenn Angreifer Authentifizierungsdaten dazu nutzen, Gelder auf ein eigenes Zielkonto zu überweisen.

Reputationsrisiken

Aus den genannten Risiken entstehen der Behörde Reputationsrisiken: Denn Bürger werden von staatlichen Stellen erwarten, dass diese jederzeit ein verlässliches und sicheres Online-Angebot zur Verfügung stellen. In diese Erwartungshaltung werden sie die vom staatlichen Online-Angebot genutzten Zahlungsdienste mit einschließen.

Daher werden zahlreiche Bürger und gegebenenfalls auch die Medien Mängel im Online-Zahlungsverkehr eines staatlichen Online-Angebots der Behörde anlasten, unabhängig davon, ob die Behörde rechtlich und faktisch den Mangel zu verantworten hat oder nicht. Für Behörden ergibt sich also die besondere Situation, dass ihnen – im Gegensatz zu anderen Betreibern von Online-Shops – auch dann Reputationsrisiken entstehen, wenn ein von ihnen genutzter lizenzierter Zahlungsdienstleister Sicherheitslücken aufweist.

Zahlungsdienstregulierung heute

Mindestanforderungen an das Risikomanagement (MaRisk)

In Deutschland wickeln Banken und Sparkassen den Großteil des Zahlungsverkehrs ab. Daneben gibt es so genannte Zahlungsinstitute und E-Geld-Institute. Alle diese kontoführenden Zahlungsdienstlei-

ster unterstehen der Aufsicht durch die Bundesanstalt für Finanzdienstleistungsaufsicht (BaFin). Sie müssen über eine ordnungsgemäße Geschäftsorganisation und ein angemessenes Risikomanagement verfügen (§ 25 a KWG), insbesondere auch für ausgelagerte Aktivitäten (§ 25 b KWG).

Die BaFin hat ihre Erwartungshaltung zur Umsetzung der §§ 25 a und 25 b KWG im Rundschreiben „Mindestanforderungen an das Risikomanagement" (MaRisk) präzisiert. Die Zahlungsdienstleister haben die MaRisk einzuhalten und werden auf ihre Einhaltung geprüft.

Mindestanforderungen an die Sicherheit von Internetzahlungen (MaSI)

Durch die MaRisk ist ein Ordnungsrahmen für die Geschäftsorganisation, insbesondere aber auch für die IT-Sicherheit von Zahlungsdienstleistungen vorgegeben. Für Online-Zahlungsdienste hat die BaFin 2015 ihre Anforderungen im Rundschreiben „Mindestanforderungen an die Sicherheit von Internet-Zahlungen" (MaSI) weiter konkretisiert.

Die MaSI basieren auf den Ergebnissen einer Arbeitsgruppe der Europäischen Zentralbank und der Europäischen Bankregulierungsbehörde EBA, den „Guidelines on the Security of Internet Payments". Diese Guidelines werden in den meisten europäischen Mitgliedsstaaten angewendet, jedoch nicht in allen. Will eine Behörde sich auf die im Folgenden dargelegten Anforderungen verlassen, dann ist es im europäischen Kontext möglich, die Compliance zu den „Guidelines on the Security of Internet Payments" als Kriterium zu verwenden.

Technisch-organisatorische Auswirkungen von MaRisk und MaSI

Durch die MaRisk wird unter anderem sichergestellt, dass Banken und Zahlungsdienstleister (ZDL), die der Aufsicht der BaFin unterliegen, die folgenden Anforderungen erfüllen:

_____ Die IT-Prozesse und IT-Systeme sind zum Zweck der Verfügbarkeit, Integrität, Vertraulichkeit und Authentizität der Daten auf gängige Standards abzustellen, zum Beispiel die Standards des BSI oder ISO 27001.

_____ Es sind Regelprozesse für die Entwicklung, Tests, Abnahme und Übergabe in die Produktionsumgebung erforderlich.

_____ Die Trennung von Test- und Produktionssystemen ist dabei einzuhalten.

_____ Die ZDL benötigen ein Notfallmanagement mit Geschäftsfortführungs- und Wiederanlaufplänen, Kommunikationskonzept und regelmäßigen Notfalltests.

Die MaSI stellen darüber hinaus weitere, für Online-Zahlungen spezifische Anforderungen.

Vor Auslösung von Zahlvorgängen hat eine starke Kundenauthentifizierung zu erfolgen – das bedeutet: Die Legitimität der Zahlungsauslösung wird anhand zweier Authentisierungselemente überprüft, die aus zwei der drei Kategorien Besitz, Wissen und Inhärenz (Biometrie) gewählt sind. Mindestens einer der Faktoren muss dabei gegen Replay-Attacken sicher ausgestaltet sein.

Tabelle 1: Konsequenzen für Behörden-Online-Angebote aus der Nutzung von Zahlungsdiensten gemäß MaSI / EBA GL

Zahlungsdienste gemäß MaSI bzw. EBA GL...	Für Behörden-Online-Angebote bedeutet das:
...unterliegen einem Risikomanagement, welches Sicherheitsbedrohungen laufend überwacht, die eingesetzten technologischen Lösungen, Auslagerungen und die technische Umgebung der Kunden berücksichtigt.	Der Zahlungsdienst unterliegt einem spezifischen IT-Sicherheits- bzw. IT-Risikomanagement.
… unterliegen einer Vorfallsüberwachung.	Der Zahlungsdienst reagiert auf Vorfälle.
… haben für schwerwiegende Sicherheitsvorfälle ihre Zusammenarbeit mit Strafverfolgungsbehörden geregelt und verpflichten auch die Händler zur Kooperation.	Bei Hacker-Angriffen und Phishing-Kampagnen werden die zuständigen polizeilichen Dienststellen vom Zahlungsdienstleister rechtzeitig eingeschaltet.
… stellen die Rückverfolgbarkeit von Transaktionen sicher.	Im Streitfall ist nachvollziehbar, welche Transaktionen wie erfolgt sind.
… setzen Betrugspräventionslösungen ein.	Das Risiko von Schäden durch betrügerische Zahlungsauslösungen sinkt.
… identifizieren ihre Kunden im Einklang mit den Geldwäschepräventionsvorschriften.	Im Streitfall ist nachvollziehbar, dass der Bürger die richtige Identität angegeben hat.
… informieren ihre Kunden umfassend und fortlaufend über den sicheren Gebrauch des Zahlungsdienstes.	Die Bürger gehen sicherer mit der Online-Bezahlung vor.

Zum Beispiel wäre die Kombination PIN und ChipTAN zulässig.

Schwächere Authentisierungsmechanismen sind für bestimmte Ausnahmefälle zulässig: Zum Beispiel können durch Kunden definierte White-Lists von Zahlungsempfängern genutzt werden. Auch darf bei Überweisungen, die zwischen Konten innerhalb desselben Zahlungsdienstleisters erfolgen, auf eine starke Kundenauthentifizierung verzichtet werden, sofern dies durch eine auf die Transaktion bezogene Risikoanalyse gerechtfertigt ist.

Die MaSI fordern für die Zahlungsdienste zudem eine Reihe spezifischer Sicherheitsmaßnahmen. Diese betreffen auch die technische Ausgestaltung des Zahlungsdienstes in Entwicklung und Betrieb sowie das interne IT-Risikomanagement des Zahlungsdienstleisters. Andere Aspekte betreffen die Vertragsgestaltung mit dem Online-Händler: Der Zahlungsdienstleister wird dazu aufgefordert, sofern notwendig den Online-Händler zu eigenen IT-Sicherheitsmaßnahmen zu verpflichten. Aus Sicht einer Behörde ist dies positiv – denn sie hat somit eine Grundlage, vom Zahlungsdienstleister konkrete Vorgaben für notwendige eigene IT-Sicherheitsmaßnahmen einzufordern.

Regulierung von morgen: PSD 2

Am 08. Oktober 2015 hat das Europäische Parlament die überarbeitete Zahlungsdiensterichtlinie „Payment Services Directive 2“ (PSD 2) erlassen, die durch Umsetzung in nationales Recht ab 2017 wirksam wird. Ziel ist, dass Zahlungsdienste sicherer werden, Verbrauchern eine größere Auswahl von Zahlungsdiensten zur Verfügung steht und das Zahlungsdiensterecht mit neuen Entwicklungen Schritt hält.

Die PSD 2 reguliert zwei neue Arten von Zahlungsdienstleistern, nämlich Zahlungsauslösedienste und Kontoinformationsdienste. Diese „Dritten Zahlungsdienstleister“ führen keine Konten, sondern greifen im Auftrag eines Kunden auf ein bestehendes Online-Zahlungskonto bei einem kontoführenden Zahlungsdienstleister zu.

Kunden erhalten durch die PSD 2 das Recht, über einen dritten Zahlungsdienstleister ihrer Wahl auf ihre Online-Zahlungskonten zuzugreifen, unabhängig davon, ob Verträge zwischen dem dritten und dem kontoführenden Zahlungsdienstleister bestehen.

Zahlungsauslösedienste initiieren Zahlungsflüsse zwischen kontoführenden Zahlungsdienstleistern, halten selbst jedoch keine Gelder. Sie dürfen personalisierte Sicherheitsmerkmale des Zahlers entgegennehmen (z. B. PIN und TAN), sind aber verpflichtet sicherzustellen, dass diese keinem Dritten außer dem kontoführenden Zahlungsdienstleister bekannt werden. Alle anderen Informationen über den Zahler dürfen nur dem Zahlungsempfänger und nur mit ausdrücklicher Zustimmung des Zahlers bereitgestellt werden.

Der dritte Zahlungsdienstleister muss sich gegenüber dem kontoführenden Zahlungsdienstleister identifizieren und mit dem kontoführenden Zahlungsdienstleister, dem Zahler und dem Zahlungsempfänger auf sichere Weise kommunizieren. Er darf keine sensiblen Zahlungsdaten des Zahlers speichern und vom Zahler keine anderen als die für das Erbringen des Zahlungsauslösedienstes erforderlichen Daten verlangen und Daten nicht für andere Zwecke verwenden oder speichern.

Risiko	Mögliche Maßnahmen der Behörde	Mögliche Maßnahmen beim ZDL der Behörde	MaRisk	MaSI	PSD 2
Kunde kann Zahlungsart nicht nutzen	Angebot vieler verschiedener Zahlungsarten	Nutzung von Standard-Schnittstellen des Kunden-Zahlungsdienstleisters	–	–	+/?
Ausfall des Zahlungsdiensts	Notfallmanagement, Angebot alternativer Zahlungsdienste	Notfallmanagement	+	+/–	?
Diebstahl personenbezogener Daten	Minimierung der Weitergabe personenbezogener Daten, Einfordern eines Informationssicherheitsmanagements beim Zahlungsdienstleister	Informationssicherheitsmanagement	+	+	+
		Privacy-by-design	–	+	+/?
		Besonderer Schutz sensibler Zahlungsdaten	–	+	+
		Härtung von Servern	–/(+)	+	+/?

Tabelle 2: Erwartete Maßnahmen beim Zahlungsdienstleister (ZDL) von Behörden aufgrund verschiedener Regelwerke

Unmittelbar nach Eingang des Zahlungsauftrags von einem Zahlungsauslösedienstleister muss der kontoführende Zahlungsdienstleister diesem alle Informationen über die Auslösung und Ausführung des Zahlungsvorgangs mitteilen.

Kontoinformationsdienste ermöglichen Kunden eine aggregierte Sicht auf die eigenen Kontodaten, die bei kontoführenden Zahlungsdienstleistern vorliegen. Ähnlich wie für Zahlungsauslösedienste stellt die PSD 2 verschiedene Anforderungen, auf die hier nicht im Einzelnen eingegangen wird.

Europäische Bankenaufsichtsbehörde

Die PSD 2 beauftragt die Europäische Bankenaufsichtsbehörde (EBA), technische Regulierungsstandards zu erarbeiten, welche die Anforderungen an die Sicherheitsmaßnahmen für die Kommunikation und die Authentifizierungsmechanismen bestimmen. Ziel ist dabei, die Vertraulichkeit und die Integrität der personalisierten Sicherheitsmerkmale der Zahlungsdienstnutzer zu schützen.

Die EBA soll weiterhin Anforderungen an gemeinsame und sichere offene Standards für die jeweilige Kommunikation zwischen den Zahlern, den kontoführenden und den dritten Zahlungsdienstleistern definieren. Somit sollen die Schnittstellen zwischen kontoführenden und dritten Zahlungsdienstleistern unabhängig von der EBA in Form öffentlich verfügbarer Standards gesetzt werden, dabei aber Anforderungen genügen, welche die EBA noch definiert.

Wer diese Standards setzt, ist noch unklar – ebenso, wie die Durchsetzung der Anforderungen der EBA praktisch geschieht. Für Online-Shop-Betreiber ist dies insofern von Belang, als sie bei der Beschaffung einer Zahlungslösung zukünftig darauf achten müssen, welche Schnittstellenstandards die Lösung unterstützt.

Noch ist unklar, wie die EBA diese Aufgabe lösen wird, zumal einige der gesetzlichen Aufträge der PSD 2 in einem Spannungsverhältnis stehen. In der Praxis kann es daher durchaus Unterschiede im Sicherheitsniveau der verschiedenen Zahlungslösungen geben, die aber zumindest ein gemeinsames Grundsicherheitsniveau nicht unterschreiten.

Die PSD 2 ist eine stärkere Rechtsgrundlage für die bestehenden Anforderungen an die Sicherheit der Online-Zahldienste kontoführender Zahlungsdienstleister. Je nachdem, wie die EBA ihren Auftrag ausführt, die PSD 2 zu konkretisieren, werden auch noch weitere Anforderungen hinzukommen.

Risk Mitigation – heute und morgen

Tabelle 2 gibt einen Überblick darüber, inwiefern Maßnahmen, die aus der MaRisk, den MaSi oder der PSD 2 folgen, Risiken im behördlichen Online-Zahlungsverkehr entgegenwirken. Dabei ist zu beobachten:

_____ Aus den MaRisk ergibt sich Grundsicherheitsniveau für kontoführende Zahlungsdienstleister mit Anforderungen an IT-Sicherheitsmanagement, IT-Betrieb und IT-Entwicklung sowie Notfallmanagement. Durch die MaSI werden zahlungsverkehrsspezifische Anforderungen im Online-Angebot der kontoführenden Zahlungsdienstleister ergänzt.

_____ Zahlungsdienstleister außerhalb Deutschlands, welche die „EBA Guidelines for the Security of Internet Payments“ einhalten, werden über ein IT-Sicherheitsmanagement verfügen sowie die gleichen für den Zahlungsverkehr spezifischen Anforderungen wie die MaSI erfüllen.

_____ Durch die PSD 2 werden die für den Zahlungsverkehr spezifischen Anforderungen auch für die dritten Zahlungsdienstleister eingeführt. Welches Grundsicherheitsniveau diese im Verbund mit den kontoführenden Zahlungsdienstleistern erreichen, ist heute aber noch unklar.

Auswirkungen auf Online-Angebote

Standard für Online-Angebote von Behörden ist das von der Bundesverwaltung angebotene Zahlungssystem ePayBL. Die zurzeit darin angebotenen Komponenten entsprechen klassischen Bankdienstleistungen (Lastschrifteinzug, Zahlung auf Rechnung, SEPA-Lastschrift, Kreditkarte) oder unterliegen als Online-Angebot von Banken den MaRisk beziehungsweise der MaSI (Nutzung des Online-Banking über „giropay“). Eine Behörde, die ePayBL nutzt, wird also davon ausgehen, dass die hier angesprochenen Fragestellungen bereits adressiert sind beziehungsweise bei künftigen Erweiterungen von ePayBL angemessen berücksichtigt werden.

Für die Sicherheit der Online-Angebote von Behörden ergeben sich durch die MaSI beziehungsweise die „EBA Guidelines for the Security of Internet Payments“ folgende Konsequenzen:

_____ Der Zahlungsdienstleister wird über ein IT-Sicherheits- beziehungsweise IT-Risikomanagement für den Zahlungsdienst verfügen, also über kompetente Ansprechpartner für Rückfragen.

_____ Der Zahlungsdienstleister wird die Behörde über erforderliche IT-Sicherheitsmaßnahmen für die Nutzung des Zahlungsdiensts im Online-Shop informieren.

_____ Die regulatorisch geforderten Sicherheitsmaßnahmen beim Zahlungsdienstleister erzeugen ein Mindestmaß an IT-Sicherheit für den genutzten Zahlungsdienst.

Soll ein Zahlungsdienst genutzt werden, so ist es also wichtig, auf die Einhaltung dieser Regulierung zu achten. Wo diese nicht durch die Aufsichtsbehörden gefordert ist (bei Staaten außerhalb der EU, aber auch bei einigen Mitgliedsstaaten), müssen entsprechende Regelungen vertraglich vereinbart werden. Dies muss aber schon bei der Ausschreibung berücksichtigt werden.

Ausblick

In Summe ergeben sich durch die aktuelle und kommende Zahlungsdiensteregulierung für Betreiber von Online-Shops erhebliche Vorteile. Insbesondere wird Betreibern von Online-Shops durch die PSD 2 weitgehende Rechtssicherheit bei der Nutzung von Zahlungsauslösediensten gewährt.

Die regulatorischen Vorgaben sollen das Sicherheitsniveau des Online-Angebots insgesamt stärken und insbesondere Betrug im Internet vorbeugen. Ob aber tatsächlich auf diese Weise ein angemessenes Mindestmaß an IT-Sicherheit aller Online-Zahlungsdienstleister garantiert wird, hängt davon ab, inwiefern europaweit ein effektives Aufsichtsregime herrscht. Weiterhin ist wesentlich, inwieweit die EBA in ihrer Konkretisierung der PSD durch technische Regulierungsstandards die richtigen Anforderungen setzt.

Wie aufgezeigt, sind staatliche Stellen aber auch dann Reputationsrisiken ausgesetzt, wenn ein in ihrem Online-Angebot genutzter Zahlungsdienstleister Sicherheitslücken aufweist – ob dieser lizenziert ist oder nicht. Unabhängig von der geltenden Regulierung bleibt es also erforderlich, die eigenen Sicherheitsanforderungen mit dem durch die Regulierung eingeforderten und vom Zahlungsdienstleister gebotenen Sicherheitsniveau abzugleichen. ■

Trau, schau, wem – oder was?

Elektronische Zahlungsdienste – Sicher! Aber wie?

Beschaffer von elektronischen Zahlungsdiensten bei Bundesbehörden können häufig nicht abschätzen, inwieweit der Dienst ihrem Sicherheitsbedarf entspricht. Im folgenden Beitrag werden Anforderungen an die Beschaffung eines Zahlungsdienstes aus Sicht des Informationssicherheits-Managements (ISMS) des Bedarfsträgers erläutert.

Von Dietmar Bremser, BSI

Im Vorfeld der Einführung eines elektronischen Zahlungsverfahrens müssen zwischen dem Hersteller und Beschaffer folgende wesentliche Anforderungen abgeklärt werden: :

_____ Welcher konkrete Sicherheitsbedarf der interessierten Parteien (Stakeholder) des Beschaffers wurde vom Hersteller antizipiert und im Produkt integriert?

_____ Wie wird der Sicherheitsbedarf des Beschaffers in der Produktentwicklung aufrechterhalten?

_____ Welche Zusicherungen kann der Hersteller geben?

In der IT-Sicherheitsbranche sind viele Methoden etabliert, um den Sicherheitsbedarf geeignet festzustellen und dauerhaft zu sichern. Dazu gehören im Wesentlichen Produkt- oder Organisationszertifikate.

Eine Produktzertifizierung nach Common Criteria (CC) prüft die Korrektheit und Effektivität der Sicherheitsfunktionen eines Produkts mit steigender Prüfstufe (Evaluation Assurance Level, EAL) von EAL 1 bis 7 umfassender. Die Entwicklungsumgebung eines Herstellers wird beispielsweise ab EAL 3 untersucht.

Des Weiteren muss der Beschaffer das Zertifikat dahingehend prüfen, welcher Sicherheitsbedarf vom Produkthersteller antizipiert wurde und welche Produktbestandteile diesen Bedarf nachweislich erfüllen. Nach CC zertifizierte Smartcards und Lesegeräte kommen im Bereich der Kartenzahlungen zum Einsatz.

Die Konzeption und Umsetzung der Prozesse und Struktur eines ISMS kann mit einem Organisationszertifikat, zum Beispiel ISO 27001 auf Basis IT-Grundschutz, testiert werden. Allerdings müssen die Restrisiken der dort eingesetzten Produkte transparent gemacht werden.

Allerdings werden zahlreiche elektronische Zahlungsverfahren von Zahlungsdienstleistern abgewickelt, die weder Karten ausgeben noch das klassische Bankgeschäft anbieten. Diese Anbieter haben seit 2015 die „Mindestanforderungen an die Sicherheit von Internetzahlungen“ (MaSI) der Bundesanstalt für Finanzdienstleistungsaufsicht (BaFin) zu beachten. Davon ausgenommen sind zum Beispiel Kleinbeträge unter 30 € oder über Browser geführte Zahlungen.

Dem Beschaffer solcher Zahlungsdienste verbleibt die Aufgabe, die Zusicherungen eines Zahlungsdienstleisters zum „gelieferten“ Sicherheitsniveau mit seinem „benötigten“ Niveau abzugleichen.

Der Standard ISO 27001 liefert seit 2013 mit der Forderung nach „Prinzipien zur sicheren Systementwicklung“ bei Eigen- (Control A.14.2.5) oder Fremdentwicklung (A.14.2.7, A.15) einen vielversprechenden Ansatz. Ausgehend von diesen Controls werden wesentliche Fragen eines Beschaffers an einen Zahlungsdienstleister erarbeitet und ein Vorgehen zum Aufbau sicherer Zuliefererketten nach ISO 21827 vorgestellt.

Anforderungen des Beschaffers

Interessierte Parteien einer Bundesbehörde sind vor allem die elektronisch zahlenden Bürger, die kontoführenden Institute und die Zahlungsdienstleister sowie das eigene Rechnungswesen und IT-Referat. Sie agieren anhand von Berechtigungsmerkmalen mit dem elektronischen Zahlungsdienst. Für die Bewertung des Informationssicherheitsmanagers sind daher nicht nur das Zugangsmedium des Bürgers, die Implementierung des Shops und seiner Schnittstellen relevant, sondern auch die an den Shop angeschlossenen Zahlungsdienste.

Das primäre Schutzgut sind aus Sicht des ISMS und der MaSI die Zahlungsdaten des Bürgers, wozu seine Authentifizierungsdaten, personenbezogenen Daten sowie die damit verbundenen Transaktionsdaten gehören. Personenbezogene Daten berühren den Datenschutz und erfordern mindestens einen hohen Schutzbedarf.

Auch wenn die Behörde die Zahlungsabwicklung einem Zahlungsdienstleister überlässt und keine Zahlungsdaten in ihrem Shop erhebt oder verarbeitet, sind Aggregationseffekte zu berücksichtigen. Dieser entsteht, wenn ein Dienstleister über den Verwaltungsakt einer Behörde Zugang zu Zahlungsdaten, der Zahlungsaufforderung und Kontoinformationen des Bürgers erlangt. Entscheidend ist, ob der Bürger eine dauerhaft vertragliche Bindung zu diesem Zahlungsdienstleister hat. Hat der Bürger keine dauerhafte vertragliche Bindung, so sind seine Sicherheitsanforderungen von der Behörde verstärkt zu priorisieren.

Ferner ist beim Einkauf eines Systems wie einem elektronischen Zahlungsdienst auf zwei Aspekte zu achten:

_____ Die Dokumentation und Umsetzung definierter Sicherheitsanforderungen des Beschaffers in der Lieferkette durch den Lieferanten sowie die Prüfung durch den Beschaffer, wenn der Lieferant Zugriff auf Werte der Organisation hat.

_____ Die Umsetzung und Prüfung der Sicherheitsanforderungen des Beschaffers im Lebenszyklus eines Systems durch den Hersteller samt Prüfung durch den Beschaffer.

Die erste Anforderung ergibt sich aus Control A.15.1.1 und A.15.1.2 der ISO 27001:2013, wobei auch Unterauftragnehmer einzubeziehen sind (A.15.1.3). Die regelmäßige Prüfung von Unterauftragnehmern formuliert A.15.2.1. Diese Anforderungen werden auch im IT-Grundschutz-Baustein „Out-Sourcing“ thematisiert (vgl. [1]).

Die zweite Anforderung zur Überwachung und Prüfung eines fremdentwickelten Systems durch den Beschaffer schreibt A.14.2.7 fest: Der Systemhersteller sollte dann die Controls A.14.2 umsetzen – im Besonderen Regeln und Prozesse zur sicheren Systementwicklung (A.14.2.5). Diese Maßnahmen betreffen jegliche Zahlungsdienste, Zahlungsverkehrsplattformen als Summe verschiedener Zahlungsdienste oder Online-Shops.

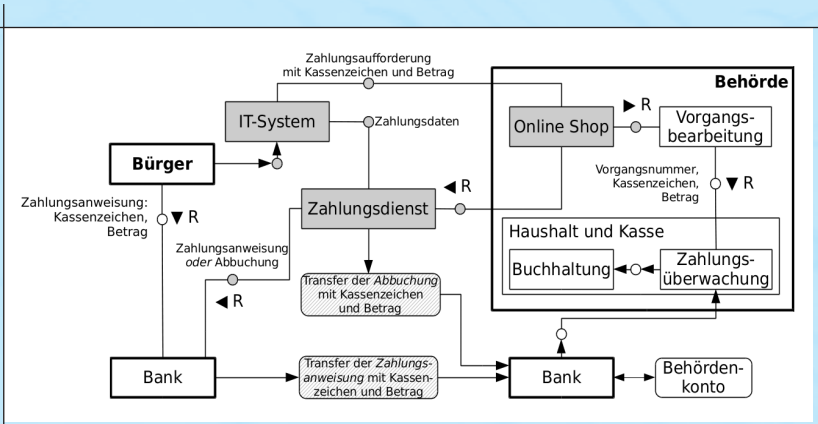

Abbildung 1: Beteiligte Parteien, Komponenten und Beziehungen eines elektronischen Zahlungsdienstes

Die IT-Grundschutz-Bausteine „Webanwendungen“, „Web-Services“ und die BSI-Leitfäden zur Entwicklung sicherer Webanwendungen [2] empfehlen sich für das Anforderungsmanagement und den Betrieb elektronischer Zahlungsdienste, sie bilden den Control A.14.2.5 unvollständig ab.

Was aber ist eine „sichere Systementwicklung“ im Sinne der ISO 27001:2013 und wie ist sie zu evaluieren?

Zusicherungen des Zahlungsdienstleisters

Die Standard ISO 21827 „Systems Security Engineering“ (SSE-CMM) [3] empfiehlt „Security by Design“, also die Integration von Risikostrategien und Sicherheitstechniken in die Systementwicklung und die Entwicklungsumgebung.

Die CC ähneln in vielen Prüfaspekten der ISO 21827 sehr stark, allerdings befassen sich die CC umfassender mit dem IT-Produkt. Die ISO 21827 konzentriert sich aufgrund des Projektcharakters und der Individualität einer Systementwicklung auf zwischen Hersteller und Anwender verzahnte Entwicklungs- und Betriebsprozesse, die nach einem Reifegradmodell geprüft werden können. Damit liefert der Standard adäquate Anforderungen zur Evaluierung von Entwicklungsprojekten, wie sie von der ISO 27001:2013 gefordert werden.

Der Standard nennt unter dem Aspekt „Security Engineering“ elf Basispraktiken (PA01 bis PA11), die als allgemeine Grundsätze im gesamten Lebenszyklus eines Sicherheitssystems angewandt werden. Das „Systems Engineering“ umfasst elf Reifepraktiken (PA12 bis PA22). Diese erweitern, auf die Prozesse und Organisation des Herstellers angewandt, die Basispraktiken und gewährleisten die konsistente, gleichbleibende Herstellung und Bereitstellung von Sicherheitstechniken und steigender Qualität über den gesamten Lebenszyklus eines Systems.

Setzt die Organisation alle Basispraktiken um, erreicht sie den Reifegrad 1. Der Reifegrad 3 erfordert wohldefinierte und koordinierte Prozesse. Organisationen mit kontinuierlichen Verbesserungsmaßnahmen erreichen Reifegrad 5.

„Security by Design“ erfordert die Kooperation des Herstellers mit dem Anwender im Lebenszyklus des Systems (vgl. Abb. 2): Beide erarbeiten gemeinsam die Sicherheitsanforderungen an das zu entwickelnde System. Der Hersteller setzt die Sicherheitsanforderungen in einer sicheren Entwicklungsumgebung um und führt ein Verzeichnis der Sicherheitsanforderungen, seiner Entwicklungsprozesse und -umgebung, Verbesserungsprozesse sowie der Test- und Betriebsparameter. Der Hersteller weist dem Anwender die Einhaltung der Anforderungen nach und unterstützt den Beschaffer beim Betrieb, der Wartung und Verbesserung des Systems.

Ein Beschaffer kann sich auf diese Weise bei der Systemevaluierung auf folgende Praktiken konzentrieren:

- die Dokumentation der von einem Produkt erfüllten Sicherheitsanforderungen,
- die Systembeschreibung einschließlich der Maßnahmen für den Systembetrieb,
- die Dokumentation der Entwicklungsumgebung, im Besonderen des Konfigurationsmanagements, sowie
- die Zusicherungen zur Qualitätssicherung des Systems, also Wartung und Weiterentwicklung.

Besonderes Augenmerk sollte auf das Konfigurationssystem gelegt werden: In diesem sind Konfigurationsobjekte, also die Dokumentationen und Aufzeichnungen des Entwicklungsprozess abgelegt. Dazu gehören Systembeschreibungen und -konfigurationen, versionierte Quelltexte, Testnachweise und Zugriffsprotokolle. Ein Konfigurationssystem soll darstellen,

- wie Produktanforderungen in den Lebenszyklus eingesteuert werden,
- welche technischen Abhängigkeiten sowie technischen und organisatorischen Anforderungen von der Einsatzumgebung des Produkts zu erfüllen sind,
- wie die Entwicklungsumgebung physisch geschützt wird und wie Zugriffsrechte der Entwickler auf den Quellcode festgelegt, zugewiesen und durchgesetzt werden,

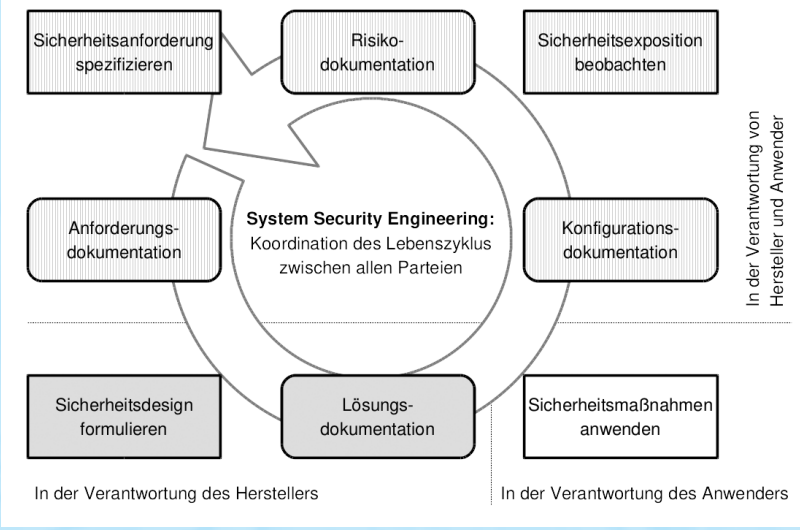

Abbildung 2: Lebenszyklus im System-Security-Engineering

_____ wo die Dokumentation, Systemkonfiguration und der Quelltext in der Entwicklungsumgebung geschützt abgelegt wird,
_____ welche Werkzeuge bei der Entwicklung und Schwachstellenbehebung eingesetzt werden,
_____ welche Leitlinien und Sicherheitsvorgaben von den Entwicklern eingehalten werden,
_____ welche Prozesse und Werkzeuge zum Test und zur Schwachstellenbehebung verwendet werden,
_____ wie das System und seine Aktualisierungen ausgeliefert werden und
_____ wie das Zusammenspiel der Systemkomponenten getestet wird.

Vorrangiges Ziel der sicheren Systementwicklung ist die Wahrung der Integrität und Vertraulichkeit der Konfigurationsobjekte in der Entwicklungsumgebung. Fremdleistungen, die der Erfüllung der Sicherheitsanforderung dienen, sind vom Hersteller daher ebenso zu dokumentieren.

Aus dem Konfigurationssystem generiert der Systementwickler Anleitungen für den Anwender, aus denen die Schutzziele und Anforderungen für einen sicheren Betrieb des Produkts hervorgehen:
_____ die Beschreibung der technischen Systemabhängigkeiten sowie technischen und organisatorischen Anforderungen der operativen Einsatzumgebung,
_____ die notwendigen Einstellungen bei der Anpassung und Installation des Produkts,
_____ die Anforderungen an das Rollen- und Berechtigungskonzept für den Anwender, seine Kunden und eventuelle externe Dienstleister,
_____ die Anforderungen an die Datenverarbeitung und -sicherung sowie das Schlüsselmaterial für temporär, dauerhaft gespeicherte und übertragene Daten,
_____ die technischen und organisatorischen Hinweise für die Produktwartung und

Tabelle 1: Beispielhafte Prüffragen für potenzielle Lieferanten

Prüfgegenstand	Praktik	Leitfragen	Prüfergebnis
Dokumentation der Sicherheitsanforderungen			
Risikobericht	PA03, PA13	Welche Risiken wurden für die Entwicklung und den Betrieb des Systems identifiziert? Wie wurden diese bewertet?	1 – angewandt? 2 – planvoll umgesetzt? 3 – koordiniert? 4 – qualitätsorientiert? 5 – qualitätsgesichert?
Sicherheitsannahmen für den Betrieb	PA10	Wie fügt sich das Produkt in die Sicherheitsleitlinie des Beschaffers ein? Dazu gehören gesetzliche und technische Anforderungen an die Organisation und Einsatzumgebung.	...
Beschreibung des Systems			
Systemhandbuch	PA01, PA09, PA06	Welche Sicherheitsleistung erbringt das Produkt in der Betriebsumgebung, d. h. welchen Risiken begegnet es? Welche Sicherheitsmaßnahmen sind in der Betriebsumgebung des Anwenders einzuhalten?	...
Dokumentation der Entwicklungsumgebung			
Sicherheitsmaßnahmen	PA07, PA17, PA18	Welche Sicherheitsmaßnahmen sind in der Entwicklungsumgebung des Herstellers implementiert? Wie wird das Berechtigungskonzept umgesetzt? Wie werden Berechtigungsmerkmale im System und in der Umgebung ausgetauscht?	...
Konfigurationsmanagement	PA13, PA20, PA08, PA05	Verfügt der Hersteller über ein Konfigurationsmanagement? Wie werden Schwachstellen erkannt und behoben?	...
Qualitätssicherung und Projektrisikomanagement			
Produktmanagement	PA12, PA19	Wie passt sich das Produkt und sein Hersteller an einen sich verändernden Sicherheitsbedarf des Beschaffers an?	...
Lieferketten	PA22	Für welche Systemkomponenten wurden externe Lieferanten aus welchen Gründen beauftragt? Wie werden Lieferantenbeziehungen gepflegt?	...

die Grenzen der Konfiguration hinsichtlich der antizipierten Sicherheitsanforderungen.

Die Praktiken der ISO 21827 richten sich nicht nur an den Hersteller, sondern auch an den Beschaffer. Der Beschaffer kann daher den in Tabelle 1 dargestellten Katalog an Prüffragen für potenzielle Lieferanten aus dem Standard ableiten.

Die beispielhaft aufgelisteten Prüffragen lassen erkennen, dass die Dokumentation der Sicherheitsanforderungen und des Systems als Basispraxis mindestens zu erbringen sind. Die Dokumentation der Entwicklungsumgebung und der Qualitätssicherung ergeben die Reife eines Systemherstellers. Empfohlen werden mindestens wohldefinierte Prozesse, also Reifegrad 3.

Fazit

Die Realität bei der Beschaffung von IT-Systemen sieht häufig anders aus, wenn Herstellereigenerklärungen haftungsrechtlich unkritische Eigenschaften zusichern und dem Beschaffer über AGB-Verträge Pflichten und Sicherheitsmaßnahmen zuweisen. Beschaffer mit ISO 27001:2013-konformen ISMS werden von Control A.14.2.7 und A.14.2.5 ermutigt, Hersteller und Lieferanten zu prüfen.

Die Produktzertifizierung wäre als Herstellerzusicherung das Mittel der Wahl, um die Gewährleistung von Sicherheitsanforderungen im Lebenszyklus eines Systems transparent zu machen, ist aber nicht immer durchzusetzen. ISO 21827 füllt damit die Lücke zwischen den Anforderungen der ISO 27001 an die Umsetzung einer sicheren Systementwicklung und den Aufbau sicherer Lieferantenbeziehungen.

Damit beugt die Behörde einerseits einem Reputationsschaden vor und begegnet vertraglichen Risiken mit Lieferanten. Da eine Behörde sich häufig langfristig an einen Hersteller bindet und nicht willkürlich eine Neubeschaffung anstoßen kann, ermöglicht ISO 21827 eine tiefe Integration von Produkten in die Betriebsprozesse der Behörde und andererseits der behördlichen Sicherheitsanforderungen in das Produktmanagement des Herstellers eines Zahlungsdienstes. ■

Literatur

[1] BSI, Zuordnungstabelle ISO 27001 sowie ISO 27002 und IT-Grundschutz, www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Grundschutz/Hilfsmittel/Doku/Vergleich–ISO27001–GS.pdf

[2] BSI, BSI-Leitfäden zur Entwicklung sicherer Webanwendungen, www.bsi.bund.de/DE/Publikationen/Studien/Webanwendungen/index–htm.html

[3] ISO 21827 „Systems Security Engineering“ (SSE-CMM), http://standards.iso.org/ittf/PubliclyAvailableStandards/c044716–ISO–IEC–21827–2008.zip

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
Giesecke & Devrient GmbH	STARCOS 3.6 COSGKV C1	Smartcard mit Anwendung (eHealth)	EAL4+ BSI-DSZ-CC-0976-2015 2015-12-29
genua gmbh	genugate firewall 8.0	Firewall	BSI-DSZ-CC-0890-2013-MA-01 2015-12-09
Brocade Communications Systems, Inc.	Brocade Communications Systems, Inc. FabricOS Version: 7.3.0a3	Softwarelösung einer Netzwerkkomponente	EAL2+ BSI-DSZ-CC-0969-2015 2015-12-08
genua gmbh	genuscreen 5.0	Firewall	EAL4+ BSI-DSZ-CC-0966-2015 2015-12-03
M-privacy GmbH	TightGate-Pro (CC) Version1.4 ReCoBS	Serveranwendung	EAL3+ BSI-DSZ-CC-0589-2015 2015-12-02

Hersteller/Vertreiber	Produkt	Produkt-Typ	Ergebnis ID Zertifizierungsdatum
Infineon Technologies AG	Infineon Technologies Smart Card IC (Security Controller) M5072 G11 with optional RSA v1.03.006, EC v1.03.006 and Toolbox v1.03.006 with specific IC dedicated software	Smartcard Controller	EAL 5+ BSI-DSZ-CC-0946-V2-2015 2015-11-23
Infineon Technologies AG	Infineon Security Controller M7893 B11 with optional RSA2048/4096 v1.03.006, EC v1.03.006, SHA-2 v1.01 libraries and Toolbox v1.03.006 and with specific IC dedicated software (firmware)	Smartcard Controller	EAL 6+ BSI-DSZ-CC-0879-V2-2015 2015-11-13
Infineon Technologies AG	Infineon Security Controller M5073 G11 with optional RSA2048/4096 v2.03.008, EC v2.03.008, SHA-2 v1.01 and Toolbox v2.03.008 libraries and with specific IC dedicated software (firmware)	Smartcard Controller	EAL 6+ BSI-DSZ-CC-0951-2015 2015-11-11
macmon secure GmbH	macmon, Version 4.0.9	System zur Netzwerkzugriffskontrolle (NAC)	EAL 4+ BSI-DSZ-CC-0738-2015 2015-11-09
secunet Security Networks AG	secunet eID PKI Suite Certified CA Kernel, Version 1.0.0	PKI Managementkomponente	EAL 4+ BSI-DSZ-CC-0960-2015 2015-11-06
T-Systems International GmbH	TCOS FlexCert Version 2.0 Release 1/SLE78CLX1440P	Smartcard Controller	BSI-DSZ-CC-0904-2015-MA-01 2015-11-04
Infineon Technologies AG	Infineon Security Controller M7892 B11 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 (firmware)	Smartcard Controller	EAL 6+ BSI-DSZ-CC-0782-V2-2015 2015-11-03
Infineon Technologies AG	Infineon smart card IC (Security Controller) M9900 A22 and G11, M9905, M9906 A11 with optional RSA v1.03.006, EC v1.03.006, Toolbox v1.03.006 and Flash Translation Layer V1.01.0008 libraries with specific IC dedicated software	Smartcard Controller	EAL 5+ BSI-DSZ-CC-0827-V3-2015 2015-11-03
IBM Corporation	PR/SM for IBM z13 EC GA1, Driver Level D22H	Serveranwendung	EAL 5+ BSI-DSZ-CC-0953-2015 2015-10-15
Infineon Technologies AG	SLB9665_2.0, v5.51.2098.00	Trusted Platform Module (TPM)	EAL 4+ BSI-DSZ-CC-0965-2015 2015-09-17

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
EFR GmbH	SGHv3	Smart Meter Gateway	BSI-DSZ-CC-1000

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
GSM Association	Embedded UICC Protection Profile, Version 1.1/2015-08-25	EAL 4+ BSI-CC-PP-0089-2015 2015-10-06
DBMS Working Group / Technical Community	Base Protection Profile for Database Management Systems	EAL 2+ BSI-CC-PP-0088-2015 2015-09-17

4. Vom BSI erteilte Standortzertifikate

Antragsteller	Entwicklungs-/ Produktionsstandorte	ID Ausstellungsdatum	gültig bis
NXP Semiconductors Hong Kong Limited	NXP Global Distribution Center Hong Kong	BSI-DSZ-CC-S-0055-2015 2016-01-08	2018-01-07
NedCard BV	NedCard (Shanghai) Microelectronics Co. Ltd.	BSI-DSZ-CC-S-0050-2016 2016-01-08	2018-01-07
HID Global Ireland Teoranta	HID Global Ireland Teoranta, Pairc Tionscail na Tulaigh, Baile na hAbhann, Co. Galway, Ireland (Building B1, B2, B3)	BSI-DSZ-CC-S-0056-2015 2015-11-27	2016-09-07
Advanced Semiconductor Engineering Kaohsiung Factory (ASEKH)	Advanced Semiconductor Engineering Inc. Kaohsiung Factory (ASEKH), Kaohsiung, Buildings K4, K7, K8, K10, K11, K12	BSI-DSZ-CC-S-0049-2015 2015-11-09	2017-11-08
United Microelectronics Corporation	United Microelectronics Corporation Fab 12i, No 3, Pasir Ris Drive 12, Singapore 519528	BSI-DSZ-CC-S-0048-2015 2015-10-07	2017-10-06

5. Vom BSI bestätigte Produkte gemäß Signaturgesetz (SigG)

Hersteller	Produktbezeichnung	Produkttyp	Registriernummer
ZF Electronics GmbH	Cherry SmartTerminal ST-2xxx; Firmwareversion: 6.01	Smartcardterminal Nachtrag zur Bestätigung	BSI.02124.TE.09.2010 2015-11-02

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

Zertifikatsnummer	Institution	Untersuchungsgegenstand	gültig bis
BSI-IGZ-0219-2015	WWK Lebensversicherung a.G.	Die WWK Lebensversicherung a. G., die WWK Allgemeine Versicherung AG und die WWK Pensionsfonds AG sind Teil der WWK Unternehmensgruppe. Untersuchungsgegenstand ist die Zentraldirektion der genannten Unternehmen inklusive des zugehörigen Informationsverbundes. In der Zentraldirektion werden die versicherungstechnischen Kernprozesse (Versicherungsprodukte managen, Versicherungsprodukte verkaufen, Kunden betreuen und Leistung erbringen) mit ihren Supportprozessen erbracht.	2018-12-08
BSI-IGZ-0222-2015	Babiel GmbH	Der Untersuchungsgegenstand umfasst den Geschäftsbereich Providing der Babiel GmbH am Standort Düsseldorf. Der Geschäftsbereich Providing wurde für die Produktivsysteme von Kunden und deren Anwendungen eingerichtet. Bei den Anwendungen handelt es sich um B2B-Shoplösungen sowie um datenbankbasierte CMS-Systeme mit Redaktionssystemen, Liveservern und ergänzenden Systemen, unter anderem auch Installation des GSB (Government Site Builder) sowie Coremedia, NPS/Fiona und Jahia.	2018-12-03
BSI-IGZ-0220-2015	indevis IT-Consulting and Solutions GmbH	Der Informationsverbund der indevis IT-Consulting and Solutions GmbH in München mit der Außenstelle Hamburg erstreckt sich über alle grundlegenden Dienstleistungen, die in den Geschäftsbereichen Managed Security, Managed Network und Managed Data Center Service Providing erbracht werden. Der Untersuchungsgegenstand umfasst alle für die Erbringung dieser Managed Services erforderlichen IT-Systeme und Prozesse sowie die beiden Rechenzentren einschließlich der Netzwerk- und Kommunikationsverbindungen, die den Kunden zur Verfügung gestellt werden. Nicht Gegenstand der Betrachtung sind die Anwendungen, die von den Kunden in eigener Verantwortung auf deren kundeneigenen Systemen und in deren eigenen Netzen betrieben werden.	2018-12-02
BSI-IGZ-0217-2015	Frama AG	Kernkonzept der Frama AG ist das Übertragen und Verwalten von sensiblen Informationen sowie das Verrechnen und Verwalten von geldwerten Daten und Kundenkonten. Der Untersuchungsgegenstand umfasst die Informations- und Kommunikationstechnologie, welche die Frama AG zum operativen Handling dieser Daten benötigt. Hierzu gehören Prozesse zur Post-/Finanz- und Stempelsteuerbearbeitung sowie Prozesse zur gesicherten Kommunikation. Diese stützen sich auf Prozesse zur Herstellung/Initialisierung/Verwendung von kryptografischen Schlüsseln und Modulen und Prozesse zum Betrieb des Datacenters am Standort in Lauperswil (CH).	2018-10-29
BSI-IGZ-0212-2015	KUKA Roboter GmbH	Der Untersuchungsgegenstand umfasst das Informationssicherheits-Management der KUKA Roboter und in Teilen der KUKA AG, die zentralen IT-Systeme der Anwendungsentwicklung sowie sämtliche IT- und Infrastruktur-Komponenten der KUKA Roboter GmbH, die für die Geschäftsprozesse CD-Bau und CPC genutzt werden. Innerhalb des CD-Bau-Prozesses werden kundenspezifische Images für die Roboter-Steuerungsrechner erstellt. Der integrierte und äußerst sensible Prozess CPC (Computer Protection by Certification) stellt dabei sicher, dass diese Images keinerlei Schadsoftware enthalten und über den gesamten Lebenszyklus des Steuerrechners nicht unautorisiert verändert werden können.	2018-08-19

Zertifikatsnummer	Institution	Untersuchungsgegenstand	gültig bis
BSI-IGZ-0215-2015	Fujitsu TDS GmbH	Der Untersuchungsgegenstand umfasst den IT-Verbund des Geschäftsbereichs Outsourcing & Consulting Services der Fujitsu TDS GmbH. Zum Verbund zählen alle Services, welche am Standort Neckarsulm, Neuenstadt am Kocher und Ulm (Bürostandort kein RZ-Betrieb durch FTDS) durch den Geschäftsbereich Outsourcing & Consulting Services der Fujitsu TDS GmbH betreut werden. Der IT-Verbund umfasst den Betrieb der Serversysteme und Netzwerkkomponenten der hochverfügbaren Rechenzentren an den Standorten Neckarsulm und Neuenstadt am Kocher.	2018-08-17
BSI-IGZ-0205-2015	Bundesagentur für Arbeit	Der Informationsverbund „IT-Produktion der Bundesagentur für Arbeit“ umfasst alle IT-Basisdienste, die für den Wirkbetrieb der IT-Verfahren der Bundesagentur für Arbeit (BA) unentbehrlich und damit für die gesetzlich vorgegebene, originäre Aufgabenerfüllung der BA unabdingbar sind. Der Informationsverbund wird durch die Geschäfts- und IT-Betriebsprozesse der fachanwendungsneutralen Infrastruktur-, Kommunikations-, System- und Anwendungsdienste bestimmt, die im Wesentlichen vom Geschäftsführungsbereich Produktion (GFB P) des Systemhauses der BA bereitgestellt werden. Die IT-Systeme des Informationsverbundes werden in den zentralen Rechenzentren und Räumlichkeiten der BA in Nürnberg betrieben.	2018-08-13
BSI-IGZ-0180-2015	WindMW GmbH	Der Informationsverbund ist der Leitstand der WindMW GmbH mit den zugehörigen Anwendungen, Servern, aktiven Netzkomponenten, WAN, Remote Zugang und Ersatzleitstand zum Betrieb der Kennzeichnungssysteme.	2018-08-11
BSI-IGZ-0211-2015	GISA GmbH	Der Informationsverbund der GISA GmbH umfasst das Hosting einzelner Systeme, den Betrieb von IT-Infrastrukturen mit den erforderlichen Anwendungen und/oder die Bereitstellung definierter Services. Der Untersuchungsgegenstand besteht aus den IT-Komponenten, die für den Betrieb selbst genutzter oder für Kunden zur Verfügung gestellter Anwendungen, IT-Systeme und Services als Grundversorgung notwendig sind. Er schließt die dafür erforderliche RZ-Infrastruktur an den Standorten in Halle sowie die benötigten Netzwerkdienste und die operative Netzwerkplattform ein. Bestandteile des Untersuchungsgegenstandes sind Systeme zur Bereitstellung von Datensicherungsdiensten, SAN-Systeme, Verzeichnisdienste, Server für Netzbasisdienste, die zugehörigen Netzkomponenten wie Router und Switche, Sicherheitsgateways und Zugangssysteme für einen kontrollierten Zugriff auf unterschiedliche Teilnetze sowie das zugehörige Netz- und Systemmanagement.	2018-07-12
BSI-IGZ-0214-2015	Kommunale Informationsverarbeitung Baden-Franken	Die Kommunale Informationsverarbeitung Baden-Franken (KIVBF) versorgt in Baden-Württemberg mehr als 550 Städte, Gemeinden und Landkreise mit über 5,25 Mio. Einwohnern mit IT-Fachlösungen. Dazu betreibt die KIVBF insbesondere Leistungszentren für Dienstleistungen der automatisierten Datenverarbeitung und der damit zusammenhängenden Leistungen, die Einrichtung, Wartung und Pflege von Anlagen und Programmen der automatisierten Datenverarbeitung, der Betrieb von Rechnern, die Beratung über Angelegenheiten der automatisierten Datenverarbeitung sowie die Schulung von Mitarbeitern. Der Untersuchungsgegenstand für die BSI-Zertifizierung umfasst alle für den Betrieb der Schutzzonen Server-Hosting, -Housing, Remote-Access sowie Internet und E-Mail-Anbindung notwendigen infrastrukturellen, organisatorischen, personellen und technischen Geschäftsprozesse sowie die dafür erforderlichen IT-Systeme.	2018-07-05