Moderne Beschaffung mit Berücksichtigung von IT-Security

Gabor Österreicher · Gerhard Pötzelsberger · Ernst Piller

Fachhochschule St. Pölten
{gabor.oesterreicher | gerhard.poetzelsberger | ernst.piller}@fhstp.ac.at

Zusammenfassung

Bei der Beschaffung von Software oder Hardware (mit integrierter Software) spielt IT-Security heute meist keine oder nur eine geringe Rolle. In dieser Arbeit werden Maßnahmen für die Beschaffung sicherer IT-Produkte behandelt. Im Rahmen des Projekts *ITsec.at* entstand eine Beschaffungsplattform, die beim Einkauf von Software bzw. Hardware mit integrierter Software, bei der Beauftragung zur Software Entwicklung oder auch bei der Anschaffung von Open Source Produkten die Sicherheit in den Vordergrund stellt. Die Plattform gliedert sich in drei große Bereiche: Beschaffung, Sicherheitsvorfälle und Produkte. Der Bereich Beschaffung dient dabei als Unterstützung für den Einkauf, um Sicherheitsanforderungen für ein Produkt zu formulieren. Beispielsweise können große oder öffentliche Unternehmen die ausgearbeiteten IT-Sicherheitsanforderungen in ihre Ausschreibungen übernehmen. Auch kleine und mittlere Unternehmen (KMUs) sowie Privatpersonen profitieren von der Plattform, indem sie sich allgemeingültige Sicherheitsanforderungen, konkrete Empfehlungen der Implementierungsstärken einzelner IT-Sicherheitsverfahren, sowie sicherheitsrelevante Informationen über bestimmte Produkte und Hersteller einholen können.

1 Einleitung

IT-Sicherheit ist für Unternehmen schon beim Einkauf von IT-Komponenten sehr wichtig. Sie spielt aber heute beim Einkauf von Software und Hardware (mit integrierter Software) meist keine oder nur eine geringe Rolle. Wir gehen in unserer Betrachtung von jeglichen Produkten/Komponenten aus, die Software enthalten, d.h. von der gesamten Palette an Software (Betriebssysteme, Standardsoftware, Anwendungssoftware, IT-Sicherheitsprodukte etc.) und Hardware, die Software enthält, wie alle IT-Produkte (PCs, Laptops, Smartphones, Server, Telekommunikationsgeräte, IT-Sicherheitsprodukte etc.), Produktionsmaschinen, Steuerungen, Geräte, Fahrzeuge etc. bis hin zu Produkten im Privatbereich, die heute alle für Unternehmen direkt oder indirekt eine Gefahr darstellen können. Dies gilt besonders durch die Öffnung fast aller dieser Produkte/Komponenten in den Cyberraum.

Solche Produkte/Komponenten sind gegen Angriffe aus dem Cyberraum sehr unterschiedlich resistent. Besonders gefährlich sind Angriffe, welche die Widerstandsfähigkeit des Produktes gezielt schon im Produktdesign bzw. während der Produktentwicklung untergraben, wie z.B. "schwache" Implementierung sicherer Kryptografie, vorinstallierte Hintertüren oder Spionage-Komponenten. Für solche, bewusst integrierten Schwachstellen gibt es sehr viele Beispiele, wie etwa der National Institute of Standards and Technology (NIST) Zufallszahlengenerator [Sch13], diverse Aktivitäten, die im Rahmen der "NSA Enthüllungen" veröffentlicht wurden [A$^+$13a, A$^+$13c, A$^+$13b, P$^+$13b] oder das Bullrun Programm [P$^+$13a, Wik]. Außerdem

P. Schartner (Hrsg.) · D•A•CH Security 2016 · syssec (2016) 214-223.

gibt es viele Fälle, bei denen angenommen werden kann, dass sich in importierten Produkten, welche von potentiell nicht vertrauenswürdigen Herstellern produziert wurden oder aus Staaten stammen, die auf Hersteller entsprechend Einfluss nehmen, derartige "By Design"-Schwächen befinden [Lis11, Ree12, Neu12, Kan13].

Da der Großteil der Produkte aus dem Ausland (viele davon aus Ländern außerhalb der EU) stammt, ist die Abhängigkeit Deutschlands und Österreichs von meist "unkontrollierbaren" Herstellern besonders hoch - aber auch inländische Hersteller können eine Gefahr darstellen. Es muss den Herstellern immenses Vertrauen entgegengebracht werden, dass sie korrekte, schwachstellenfreie und sichere Produkte liefern.

Der vorliegende Artikel beschreibt Ergebnisse des Projekts *ITsec.at*. Im Rahmen dieses Projekts wurden Maßnahmen für die Beschaffung sicherer IT-Produkte behandelt. Dabei entstand eine Beschaffungsplattform, die beim Einkauf von Software, Hardware mit integrierter Software und Open Source Produkten die Sicherheit in den Vordergrund stellt. Das Projekt, mit einer Laufzeit vom 01.11.2014 bis 02.12.2016, wurde von der österreichischen Forschungsförderungsgesellschaft (FFG) gefördert und im Sicherheitsforschungs-Förderprogramm KIRAS vom Bundesministerium für Verkehr, Innovation und Technologie finanziert. Konsortialführer und zentrale F&E-Stelle ist das Institut für IT-Sicherheitsforschung der Fachhochschule St. Pölten. Konsortialpartner sind das österreichische Bundeskanzleramt, Bundesministerium für Inneres (BM.I), Bundesministerium für Landesverteidigung und Sport (BMLVS), Magistrat der Stadt Wien (MA14, Informations- und Telekommunikationssysteme) und die SEC Consult Unternehmensberatung GmbH. Des Weiteren sind die ITSV (IT der Sozialversicherungsträger) und die Cyber Security Plattform der Bundesregierung Projektteilnehmer.

In dieser Arbeit beziehen sich die Begriffe "Hersteller" und "Anbieter" auf jene des Endprodukts, da diese für die Funktionalitäten dessen verantwortlich sind, und nicht auf etwaige Einzelkomponenten. Gleichermaßen werden auf der entwickelten Beschaffungsplattform ebenfalls nur Endprodukte betrachtet.

2 Themennahe Arbeiten

Durch die Öffnung in den Cyberraum stellen immer mehr Produkte direkt oder indirekt eine Gefahr für Unternehmen dar. Es gibt bereits zahlreiche Ideen und Methoden, IT-Sicherheitsanforderungen für Produkte zu etablieren. Dazu zählen zum Beispiel Sicherheitsanforderungen für die Vermeidung typischer Software Schwachstellen wie der OWASP Application Security Verification Standard (ASVS) [OWA15] oder der OWASP Secure Software Contract Annex [OWA] für in Auftrag gegebene Software Entwicklungen. Im Bereich Information über Sicherheitsvorfälle existieren beispielsweise die Schwachstellenampel des Bundesamts für Sicherheit in der Informationstechnik (BSI) [BSI], die die aktuelle Sicherheitslage in Bezug auf Sicherheitslücken in gängigen Softwareprodukten aufzeigt, sowie Warnmeldungen nationaler Computer Emergency Response Teams (CERTs). Die Cyber-Security-Plattform der österreichischen Bundesregierung erarbeitet Mindeststandards für die IT-Security von Produkten, die in weiterer Folge in eine "Procurement-Arbeitsgruppe" der ENISA (European Union Agency for Network and Information Security) einfließen wird.

Das Projekt ITsec.at geht einen Schritt weiter, indem konsolidierte Informationen für den Einkauf von sicheren softwaregestützten Produkten in Form einer Beschaffungsplattform zur Verfügung gestellt werden. Im Gegensatz zu einzelnen, im Internet verteilten Sicherheitsanforderungen soll die Beschaffungsplattform als zentrale Anlaufstelle dienen, auf der ein Benutzer

umfangreiche Informationen über die Sicherheitsaspekte findet, die vor einer möglichen Beschaffung in Betracht zu ziehen sind.

3 Maßnahmen für Beschaffung sicherer IT-Produkte

Der in der Einleitung skizzierten Abhängigkeit von Herstellern kann durch verschiedenste Maßnahmen entgegengewirkt werden. Eine kostengünstige und trotzdem sicherheitstechnisch effektive Lösung ist über eine geeignete Beschaffung der Produkte möglich. Diese umfasst eine Sammlung von Maßnahmen wie:

- Beschaffungsstrategie und Beschaffungsrichtlinien
- Anforderungskataloge für Hardware- und Software-Komponenten, inklusive Schutzbedarfsklassifikation für die Beschaffung
- Datenbank über Schwachstellen und andere sicherheitsrelevante Vorkommnisse
- Berücksichtigung des Vertrauens
- Sicherheitszertifizierungen, Sicherheitslabel, etc.
- Qualifizierte Kundenrezessionen und Testdatenbank

In den folgenden Abschnitten werden diese Maßnahmen genauer beleuchtet.

3.1 Beschaffungsstrategie und Beschaffungsrichtlinien

Bei der Beschaffungsstrategie handelt es sich in diesem Fall um Erweiterungen des Regelbereichs von üblichen IKT-Beschaffungsstrategien, damit bei der Beschaffung auch die IT-Security und Vertrauenswürdigkeit von Software und Hardware Berücksichtigung findet.

Zusätzlich zur Beschaffungsstrategie sind Beschaffungsrichtlinien zu erstellen, die bei der Beschaffung die erforderlichen Anforderungen an die IT-Security berücksichtigen. Soweit vorhanden finden hier die IT-Security-Policy eines Unternehmens und sonstige eventuell vorhandene anwendungs- oder produktbezogene IT-Security-Policies, Pflichtenhefte, interne und externe Vertragsbedingungen etc. Beachtung. Dabei spielen auch gesetzliche Vorgaben eine wichtige Rolle.

3.2 Anforderungskataloge für Software und Hardware

Um entscheiden zu können, welche Produkte sicher und vertrauenswürdig sind, wurden im Projekt Anforderungskataloge für Software- und Hardware-Komponenten entwickelt. Die IT-Sicherheitsanforderungen wurden, wo es möglich war, aus bekannten Sicherheitsstandards entnommen und gegebenenfalls konkretisiert. Die Sicherheitsanforderungen für die Vermeidung typischer Software Schwachstellen basieren auf den Anforderungskatalog für Standardsoftware des BSI [BSI14], dem OWASP Application Security Verification Standard (ASVS) [OWA15] und den CWE/SANS Top 25 Most Dangerous Software Errors [Cor11].

Die entwickelten Anforderungen decken die Bereiche IT-Sicherheit, Datenschutz und Vertrauenswürdigkeit ab. Dabei wird zwischen Standard-Software, in Auftrag gegebener Software, Hardware mit integrierter Software, sowie speziellen Kriterien für Open Source Produkte unterschieden. Die Sicherheitsanforderungen können bei der Beschaffung sowohl in Ausschreibungen, als auch als Checklisten bei einer Produktbeschaffung ohne Ausschreibung verwendet werden. Diese Anforderungen sind möglichst allgemein formuliert, sodass sie auf möglichst

alle Software-Produkte und Produkte, die Software beinhalten, zutreffen. Der Anforderungskatalog für Standardsoftware ist beispielsweise in die folgenden Kategorien gegliedert:

- Anforderungen an die Benutzerauthentifizierung
- Anforderungen an die Wahrung der Vertraulichkeit von Daten (Verschlüsselung)
- Anforderungen bezüglich Sabotage oder Spionage
- Anforderungen an die Fehlerbehandlung und das Logging
- Anforderungen an Sicherheitsupdates
- Anforderungen an den Datenschutz
- Anforderungen bei Benutzereingaben
- Anforderungen an die Konfiguration

Aufgrund des Umfangs der Anforderungen wurde eine Kurzfassung sowie eine Langfassung mit ausführlicher Erklärung entwickelt. Beispiele für einzelne Punkte aus der Kurzfassung aus der Kategorie Verschlüsselung sind wie folgt:

- Alle sensiblen Informationen werden *verschlüsselt gespeichert* und die Übertragung dieser Informationen erfolgt über *geschützte Kanäle*.
- Es werden *etablierte Algorithmen* zur Wahrung der Vertraulichkeit von Daten verwendet, die dem aktuellen Stand der Technik entsprechen und von denen keine Sicherheitslücken bekannt sind.
- Beim Einsatz kryptographischer Verfahren wird eine *empfohlene Schlüssellänge* nach aktuellem Stand der Technik eingesetzt.

Zusätzlich zu den allgemeinen IT-Sicherheitsanforderungen wurden eine Reihe von konkreten Empfehlungen ausgearbeitet, die eine notwendige Implementierungsstärke einzelner IT-Sicherheitsverfahren festlegt, wie z.B. die zu verwendende Schlüssellänge eines Verschlüsselungsalgorithmus. Diese konkreten Empfehlungen werden auf aktuellem Stand der Technik gehalten, wie z.B.:

- Bei den Blockchiffren ist der *Advanced Encryption Standard (AES)* [Fed01] der einzig empfohlene Algorithmus, in folgenden Varianten und Betriebsmodi:
  - `AES-128`, `AES-192`, `AES-256` in den Betriebsmodi Cipher-Block Chaining (CBC), Counter Mode (CTR) [D.01] oder Galois-Counter-Mode (GCM) [D.07].
  - Die empfohlene (sowie minimale) Schlüssellänge für AES sind 128 Bit. Für die Verschlüsselung von langfristig schützenswerten Informationen ist die Verwendung von AES mit einer Schlüssellänge von 256 Bit empfohlen.

Dadurch, dass die zu beschaffenden Produkte in verschiedenen Anwendungsbereichen eingesetzt werden können, ist es sinnvoll, die Anforderungskataloge und Sicherheitsempfehlungen in unterschiedliche Schutzbedarfsklassen aufzuteilen. So wurden im Projekt drei Schutzbedarfsklassen definiert: “normal”, “hoch” und “sehr hoch”.

3.3 Sicherheitsvorfälle

Während die Anforderungskataloge eine zukünftige Beschaffung abdecken, ist es weiters zweckmäßig, sich über vergangene Sicherheitsvorfälle eines Produktes oder Herstellers informieren zu können. Dies ermöglicht eine Einsicht, ob ein Hersteller transparent in der Kom-

munikation von Sicherheitsvorfällen ist, oder eine entsprechende Reaktion zeitnah erfolgt ist. Als Quelle der Sicherheitsvorfälle eignen sich dabei CERT-Warnungen und die Common Vulnerability Enumeration (CVE) Schwachstellen-Datenbank von MITRE [MIT], die alle öffentlich bekannten Sicherheitslücken listet.

3.4 Berücksichtigung des Vertrauens

Da Herstellern ein immenses Vertrauen entgegengebracht werden muss, dass sie korrekte, schwachstellenfreie Produkte liefern, gilt es zu beachten, wo Produkte entwickelt und hergestellt werden und welchen nationalen Gesetzgebungen und Datenschutzbestimmungen diese unterliegen. Um beispielsweise einer "Hintertür" in Hardware entgegenzuwirken, kann ein Vertrauenskriterium die Herkunft des Herstellers sein. Bei der Verarbeitung und Speicherung von Daten ist das Land, in dem dies durchgeführt wird, ausschlaggebend dafür, welche Behörden sich per Gesetz Zugriff auf die Daten verschaffen können. Daher ist bei einer Beschaffung von IT-Komponenten neben den sicherheitstechnologischen Aspekten auch die Vertrauenskomponente ein wesentlicher Faktor.

3.5 Sicherheitszertifizierungen

Um die Einhaltung der Anforderungskataloge und die Stärkung des Vertrauens in Produkte nach außen hin wirksam zu machen, ist auch das Thema der Zertifizierung relevant. Einerseits kann eine Zertifizierung eines Produkts z.B. nach "Common Criteria" [Com12] sicherstellen, dass die IT-Sicherheitsanforderungen erfolgreich erfüllt und getestet sind. Andererseits kann ein Hersteller auch Vertrauen für ein Produkt und in weiterer Folge für sich selbst schaffen, indem er durch eine geeignete Selbstzertifizierung die Einhaltung der vorgegebenen Sicherheitsanforderungen garantiert und Haftung für etwaige Verstöße übernimmt.

Die Zertifizierung nach Common Criteria in höheren Klassen ist aufwendig und bisher wurden nur verhältnismäßig wenige Produkte danach zertifiziert (siehe [Com]). Bei diesem Projekt wurde daher eine einfache Form der Selbstzertifizierung gewählt, die einen schnellen, kostengünstigen und unkomplizierten Weg ermöglicht, einem Beschaffer die Einhaltung der Sicherheitsanforderungen zu demonstrieren. Durch diesen Vorteil für die Hersteller ist es denkbar, dass eine Selbstzertifizierung für eine breite Produktpalette angewendet wird.

3.6 Qualifizierte Kundenrezessionen

Ein weiterer entscheidungsunterstützender Input für den Beschaffungsprozess sind qualifizierte Kundenrezessionen und eine Datenbank über Produkt-Sicherheitstests. Die qualifizierte Bewertung kann auf ähnliche Weise wie bei gängigen Bewertungsportalen mit freier Kommentarmöglichkeit umgesetzt werden, mit der Einschränkung, dass die Qualifikation der Rezensenten verifiziert wurde und die Bewertung nur den IT-Sicherheitsaspekt der Produkte betrifft. Qualifizierte Kundenrezessionen und Produkt-Sicherheitstests garantieren eine zusätzliche, herstellerunabhängige Meinungsbildung über die IT-sicherheitsrelevanten Erfahrungen mit einem Produkt.

4 Beschaffungsplattform

Damit eine IT-sicherheitsbezogene Beschaffung von Software und Hardware wie zuvor beschrieben effektiv, benutzerfreundlich und leicht verständlich einer größeren Personengruppe

zugänglich gemacht werden kann, erfolgte im Zuge des Projekts ITsec.at der Aufbau einer webbasierten Beschaffungsplattform (siehe Abbildung 1).

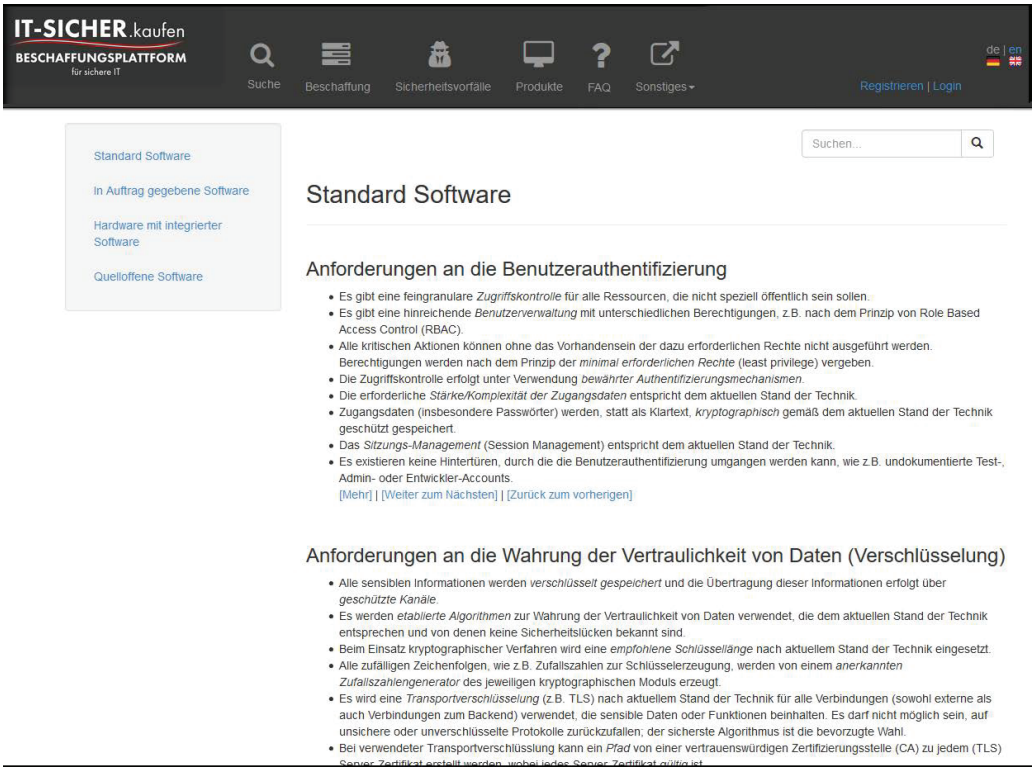

Abb. 1: Beschaffungsplattform

Die Realisierung der öffentlich zugänglichen Plattform ermöglicht den unterschiedlichen Benutzergruppen einen schnellen und umfangreichen Zugriff auf ihre jeweils benötigten Informationen. Große und öffentliche Unternehmen können die ausgearbeiteten IT-Sicherheitsanforderungen in ihre Ausschreibungen übernehmen; dies ist sowohl für die IT-Beschaffer an sich als auch für IT-Verantwortliche relevant, die den Unternehmenseinkauf hinsichtlich IT-Sicherheit unterstützen. Aber auch kleine und mittlere Unternehmen (KMUs) profitieren von der Plattform, indem sie sich allgemeingültige Sicherheitsanforderungen, konkrete Empfehlungen der Implementierungsstärke einzelner IT-Sicherheitsverfahren, sowie sicherheitsrelevante Informationen über bestimmte Produkte und Hersteller einholen können. Zusätzlich kann die von der Plattform zur Verfügung gestellte semantische Suche von jeglichen Personen, die an IT-Sicherheit interessiert sind, benutzt werden, um Informationen über Sicherheitsvorfälle und Schwachstellen einzuholen. Die dabei eingebundenen externen Quellen (siehe Kapitel 4.5) runden die breiten Möglichkeiten der Informationsgewinnung ab. Nicht zuletzt sollen auch die Hersteller/Anbieter von der Plattform profitieren, indem sie durch das Eintragen ihrer Produkte samt sicherheitsrelevanter Informationen Transparenz demonstrieren und so öffentlich Vertrauen bei ihren potentiellen Kunden erzeugen können.

Die aktuelle Version der Beschaffungsplattform besteht aus drei großen Bereichen:

- Beschaffung
- Sicherheitsvorfälle
- Produkte

Die entwickelte Beschaffungsplattform hat es nicht zum Ziel, Einfluss auf die Geschäftsprozesse eines Unternehmens zu nehmen, indem sie einen gesamten Beschaffungsprozess abwickelt. Der Inhalt der Plattform dient lediglich als Unterstützung für den Einkauf, um IT-Sicherheitsanforderungen für ein Produkt zu formulieren.

4.1 Beschaffung

Im Bereich "Beschaffung" sind die entwickelten IT-Sicherheitsanforderungen und konkreten Empfehlungen aus Kapitel 3.2 dargestellt. Die Anforderungskataloge sind in die Kategorien Standardsoftware, in Auftrag gegebene Software, Hardware mit integrierter Software und Open Source unterteilt. Bis auf Open Source gibt es für jede dieser Kategorien eine kurze Überblicks- sowie eine Langversion der Sicherheitsanforderungen. Diese Aufteilung soll sicherstellen, dass die Sicherheitsanforderungen sowohl als Checkliste, als auch als sicherheitsspezifizierende Texte in Ausschreibungen verwendet werden können und gleichzeitig die nötigen Hintergrundinformationen geliefert werden. Der Beschaffungsbereich der Plattform beinhaltet auch konkrete Empfehlungen über die notwendige Implementierungsstärke einzelner Sicherheitsverfahren.

In der Kategorie Open Source wurde ein anderer Zugang gewählt, indem unterschiedliche Bewertungskriterien und Lizenzmodelle für eine Qualitätseinschätzung beschrieben werden. Zusätzlich wird ein entsprechender Fragenkatalog zur Verfügung gestellt, um eine Bewertung und Gegenüberstellung von in Frage kommenden Softwareprodukten zu ermöglichen.

4.2 Sicherheitsvorfälle

Die Umsetzung der Maßnahme aus Kapitel 3.3 wurde im zweiten Hauptbereich der Plattform realisiert. Dieser Bereich erlaubt es, nach aktuellen oder vergangenen Sicherheitsvorfällen zu suchen, die bestimmte Produkte oder Hersteller betreffen. Dafür ist auf der Plattform eine Datenbank eingebunden, die alle aktuellen CVE-Schwachstellen von MITRE sowie die aktuellen Warnungen des österreichischen CERTs (cert.at) beinhaltet. Dadurch bietet die Plattform eine unabhängige Quelle für Information über Schwachstellen von bestehenden Produkten. Mithilfe einer Suche nach Sicherheitsvorfällen kann sich ein Beschaffer informieren, ob für ein gewisses Produkt Schwachstellen oder Warnungen existieren und wie die Reaktion des Herstellers auf diese waren. Die Schwachstellen werden ohne Bewertung und Interpretation auf der Plattform zur Verfügung gestellt. Sie dienen lediglich als Orientierungshilfe für die Transparenz eines Herstellers oder die Anfälligkeit eines bestimmten Produktes. Wenn beispielsweise ein Produkt regelmäßig Zero-Day Lücken mit hoher Kritikalität vorweist, dann ist das ein typisches Merkmal für ein anfälliges Produkt, wie es z.B. bei Adobe Flash der Fall ist.

4.3 Produkte

Der dritte Bereich der Plattform umfasst eine Sammlung von Produkten. Hier können Hersteller oder Produktanbieter – nach einmaliger Registrierung auf der Plattform – Produkte mit ihren IT-sicherheitsrelevanten Eigenschaften hinzufügen. Dafür wird die erarbeitete Checkliste von Sicherheitsanforderungen ausgefüllt und vom Unternehmen per rechtsgültiger Unterschrift bestätigt. Dies ist die Umsetzung der einfachen Form der Selbstzertifizierung aus Kapitel 3.5. Für einen Beschaffer bietet sich somit ein transparentes Bild, welche Sicherheitsanforderungen ein Hersteller bei seinem Produkt erfüllt und wofür dieser Haftung übernimmt. Das Hinzufügen von Produkten mit ihren IT-sicherheitsrelevanten Eigenschaften soll zur Steigerung des Vertrauens in einen Hersteller sowie in seine Produkte beitragen.

Des Weiteren enthält der Bereich Produkte eine Auflistung von IT-Sicherheitsprodukten mit einer Herkunftsangabe. Die Angabe der Herkunft der Hersteller soll zur Vertrauensbildung beitragen.

4.4 Schutzbedarfsklassifikation

Für einen Beschaffer gibt es auf der Plattform weiters die Möglichkeit, durch die Beantwortung weniger Fragen feststellen zu lassen, in welche Schutzbedarfsklasse der Anwendungsfall seiner Beschaffung fällt. Die Anforderungskataloge und Sicherheitsempfehlungen sowie die eingetragenen Produkte sind dabei in die drei Schutzbedarfsklassen “normal”, “hoch” und “sehr hoch” aufgeteilt, und die Anzeige kann je nach Anwendungsfall auf den passenden Schutzbedarf eingeschränkt werden. Die Schutzbedarfsklassen wurden in Anlehnung an die Schutzbedarfskategorien des österreichischen Informationssicherheitshandbuchs definiert.

Ein Beispiel für eine Frage zur Bestimmung des Schutzbedarfs ist:

- Wie sensibel sind die Daten bzw. Informationen, die verarbeitet werden?
  - Normal = Öffentliche Informationen
  - Hoch = Interne Informationen eines Unternehmens
  - Sehr hoch = Besonders schützenswerte Daten, wie z.B. medizinische Daten

4.5 Sonstiges

Zusätzlich zu den drei großen Bereichen bietet die Beschaffungsplattform eine Suche über die gesamten Inhalte der Plattform. Diese wurde als semantische Suche mit Hilfe einer speziellen “Suchmaschine” implementiert und bindet auch externe Quellen, wie z.B. den IT-Grundschutzkatalog des BSI, für eine weitere Informationsbeschaffung mit ein. Die Suche bietet auch die Möglichkeit, die Ergebnisse auf einzelne Teilbereiche der Plattform wie Anforderungskataloge, Sicherheitsvorfälle, Produkte oder externe Quellen einzugrenzen. Die durchgeführten Suchanfragen werden dabei weder gespeichert noch kommerziell ausgewertet.

Die gesamte Beschaffungsplattform steht mit Projektende im Herbst 2016 kostenlos allen Benutzern unter der URL `https://it-sicher.kaufen` zur Verfügung. Sie ist herstellerunabhängig und werbefrei. Der Betrieb und die Wartung der Beschaffungsplattform erfolgt an der Fachhochschule St. Pölten.

5 Zusammenfassung

Im Rahmen des Projekts wurden Maßnahmen für die Beschaffung sicherer IT-Produkte behandelt. Dabei entstand eine Beschaffungsplattform, die beim Einkauf von Software, Hardware mit integrierter Software, oder Open Source Produkten die Sicherheit in den Vordergrund stellt.

Die Plattform gliedert sich in drei große Bereiche: Beschaffung, Sicherheitsvorfälle und Produkte. Der Inhalt des Bereichs Beschaffung dient als Unterstützung für den Einkauf, um Sicherheitsanforderungen für ein Produkt zu formulieren. Der Bereich Sicherheitsvorfälle erlaubt es, nach aktuellen oder vergangenen Sicherheitsvorfällen zu suchen, die bestimmte Produkte oder Hersteller betreffen. Im Bereich Produkte können Hersteller oder Produktanbieter Produkte mit ihren IT-sicherheitsrelevanten Eigenschaften hinzufügen. Dafür wird die erarbeitete Checkliste von Sicherheitsanforderungen ausgefüllt.

Unterschiedlichen Benutzergruppen wird auf der Plattform ein schneller und umfangreicher Zugriff auf ihre jeweils benötigten Informationen ermöglicht. Große und öffentliche Unternehmen können die ausgearbeiteten IT-Sicherheitsanforderungen in ihre Ausschreibungen übernehmen. Auch KMUs und kleinere Organisationen profitieren von der Plattform, indem sie sich allgemeingültige Sicherheitsanforderungen, konkrete Empfehlungen der Implementierungsstärke einzelner IT-Sicherheitsverfahren, sowie sicherheitsrelevante Informationen über bestimmte Produkte und Hersteller einholen können. Zusätzlich kann die von der Plattform zur Verfügung gestellte semantische Suche von jeglichen Personen, die an IT-Sicherheit interessiert sind, benutzt werden, um Informationen über Anforderungen, Sicherheitsvorfälle und Schwachstellen oder Produkte einzuholen. Die dabei eingebundenen externen Quellen runden die breiten Möglichkeiten der Informationsgewinnung ab. Nicht zuletzt sollen auch die Hersteller/Anbieter von der Plattform profitieren, indem sie durch das Eintragen ihrer Produkte samt sicherheitsrelevanter Informationen Transparenz demonstrieren und so öffentlich Vertrauen bei ihren potentiellen Kunden erzeugen können.

6 Ausblick

Der Anforderungskatalog für die Beschaffung in der aktuellen Version der Plattform hat einen bewusst allgemeingültig gehaltenen Charakter, um ein möglichst breites Anforderungsprofil abzudecken. Es ist aber durchaus denkbar, neben diesen generischen Anforderungen branchengerechte Ergänzungen vorzunehmen, wie z.B. für das Energie- oder Gesundheitswesen. Diese Ergänzungen können verschiedene branchenspezifische Inhalte umfassen, wie z.B. gesetzliche Vorgaben, Verordnungen, Normen oder auch Zertifikate. In Österreich denken bereits unterschiedliche Gruppierungen aus den Bereichen Energie, Gesundheit oder Industrie daran, derartige Mindestanforderungen für ihre jeweilige Branche auszuarbeiten. Des Weiteren ist es geplant, den Anforderungskatalog der Plattform zweisprachig auf Deutsch und Englisch anzubieten.

Auch in anderen Teilbereichen der Plattform ist ein Input von Stakeholdern und eine darauf basierende Erweiterung denkbar und durchaus als zielführend zu bewerten. So können im Bereich Sicherheitsvorfälle weitere Datenbanken eingebunden werden, sofern diese Daten nützlich für die Benutzergruppen der Plattform sind. Ab einer entsprechenden Anzahl von abgebildeten Produkten ist es außerdem sinnvoll, qualifizierte Kundenrezessionen zu ermöglichen, wie bereits in Kapitel 3.6 angedacht. Bei entsprechender Resonanz ist auch denkbar, ein Sicherheitslabel zu erstellen, das Hersteller auf ihren Produkten anbringen können, nachdem diese in der Plattform eingetragen wurden. Nicht zuletzt sollten auch neue, themenbezogene externe Quellen aufgegriffen werden, um einer umfangreichen und möglichst vollständigen Informationsgewinnung zu genügen.

Literatur

[A+13a] J. Appelbaum et al. Die Klempner aus San Antonio. Der Spiegel, Dezember 2013. [Online; Zugriff 25-Mai-2016].

[A+13b] J. Appelbaum et al. Neue Dokumente: Der geheime Werkzeugkasten der NSA. Spiegel Online, Dezember 2013. [Online; Zugriff 25-Mai-2016].

[A+13c] J. Appelbaum et al. Otto-Katalog für Spione. Der Spiegel, Dezember 2013. [Online; Zugriff 25-Mai-2016].

[BSI] BSI. Schwachstellenampel. https://www.cert-bund.de/schwachstellenampel. [Online; Zugriff 25-Mai-2016].

[BSI14] BSI. B 1.10 Standardsoftware. IT-Grundschutz-Kataloge, 2014. [Online; Zugriff 25-Mai-2016].

[Com] Common Criteria. Certified Products. http://www.commoncriteriaportal.org/products/. [Online; Zugriff 25-Mai-2016].

[Com12] Common Criteria for Information Technology Security Evaluation. http://www.commoncriteriaportal.org/cc/, September 2012. [Online; Zugriff 25-Mai-2016].

[Cor11] The MITRE Corporation. CWE/SANS Top 25 Most Dangerous Software Errors. http://cwe.mitre.org/top25/, 2011. [Online; Zugriff 25-Mai-2016].

[D.01] Morris D. Recommendation for Block Cipher Modes of Operation: Methods and Techniques. NIST Special Publication SP800-38A, 2001.

[D.07] Morris D. Recommendation for Block Cipher Modes of Operation: Galois/Counter Mode (GCM) and GMAC. NIST Special Publication SP800-38D, 2007.

[Fed01] Federal Information Processing Standards Publication 197 (FIPS PUB 197). Advanced Encryption Standard (AES), 2001.

[Kan13] A. Kannenberg. Bruce Schneier zum NSA-Skandal: “Die US-Regierung hat das Internet verraten”. heise online, September 2013. [Online; Zugriff 25-Mai-2016].

[Lis11] K. Lischka. Hardware-Importe: US-Heimatschutz fürchtet Spionage-Viren ab Werk. Spiegel Online, Juli 2011. [Online; Zugriff 25-Mai-2016].

[MIT] MITRE. Common Vulnerabilities and Exposures. [Online; Zugriff 25-Mai-2016].

[Neu12] C. Neumann. Geheimbericht zu Huawei-Produkten: Sicherheitslücken statt Spionage. Spiegel Online, Oktober 2012. [Online; Zugriff 25-Mai-2016].

[OWA] OWASP. Secure Software Contract Annex. https://www.owasp.org/index.php/OWASP_Secure_Software_Contract_Annex. [Online; Zugriff 25-Mai-2016].

[OWA15] OWASP. Application Security Verification Standard (ASVS) 3.0, 2015. https://www.owasp.org/index.php/Category:OWASP_Application_Security_Verification_Standard_Project,

[P+13a] N. Perlroth et al. Secret Documents Reveal N.S.A. Campaign Against Encryption. New York Times, September 2013. [Online; Zugriff 25-Mai-2016].

[P+13b] L. Poitras et al. Angriff aus Amerika. Der Spiegel, Juli 2013. [Online; Zugriff 25-Mai-2016].

[Ree12] J. Reed. Proof That Military Chips From China Are Infected? Defensetec, Mai 2012. [Online; Zugriff 25-Mai-2016].

[Sch13] F.A. Scherschel. NSA-Affäre: Generatoren für Zufallszahlen unter der Lupe. heise online, September 2013. [Online; Zugriff 25-Mai-2016].

[Wik] Bullrun (decryption program). Wikipedia. [Online; Zugriff 25-Mai-2016].