Entwicklung eines Common Criteria Schutzprofils für elektronische Wahlgeräte mit Paper Audit Trail

Jurlind Budurushi, Stephan Neumann, Genc Shala, Melanie Volkamer

Security, Usability and Society
Technische Universität Darmstadt
Hochschulstraße 10
64289 Darmstadt
name.surname@cased.de

Abstract: Mit dem Urteil vom 3. März 2009 hat das Bundesverfassungsgericht die bislang in der Bundesrepublik Deutschland eingesetzten Wahlgeräte für verfassungswidrig erklärt. Grund für dieses Urteil war die fehlende Umsetzung des Prinzips der *Öffentlichkeit der Wahl*. Mit dem Urteil erklärte das Gericht jedoch nicht grundsätzlich den Einsatz elektronischer Wahlgeräte für verfassungswidrig. Im Rahmen des von der DFG geförderten Projekts 'VerKonWa' wurde das EasyVote System entwickelt, welches den Öffentlichkeitsgrundsatz durch sogenante Paper Audit Trails umsetzt. Im Rahmen dieser Arbeit berichten wir über die Erfahrung bei der Entwicklung eines Common Criteria Schutzprofils für elektronische Wahlgeräte mit Paper Audit Trails.

1 Einführung

In Deutschland waren bis zum Jahr 2005 elektronische Wahlgeräte im Einsatz. Diese sowie die entsprechende Bundeswahlgeräteverordnung wurden mit dem Urteil des Bundesverfassungsgerichts vom 3. März 2009 [Bun09] für verfassungswidrig erklärt, weil weder die Geräte noch die Verordnung mit dem Prinzip der *Öffentlichkeit der Wahl* vereinbar sind. Dieses Urteil untersagt nicht grundsätzlich den Einsatz elektronischer Wahlgeräte, solange diese mit der *Öffentlichkeit der Wahl* vereinbar sind, d.h. jeder Wähler die wesentlichen Schritte der Wahlhandlung und Ergebnisermittlung zuverlässig und ohne besondere Sachkenntnisse überprüfen kann [HVB12]. Diese Überprüfbarkeit wird in der technischen Literatur als Verifizierbarkeit bezeichnet.

Im Rahmen des von der DFG geförderten Projekts 'VerKonWa' wurde das EasyVote System entwickelt, welches den insbesondere geforderten Öffentlichkeitsgrundsatz durch sogenante Paper Audit Trails umsetzt. Für diesen Ansatz sollte im Rahmen dieser Arbeit ein Common Criteria Schutzprofil entwickelt werden, welches sicherstellt, dass die rechtlichen Vorgaben - u.a. die Öffentlichkeit der Wahl - von zukünftigen Produkten, die nach diesem Schutzprofil ervaluiert werden, umgesetzt werden. Dazu sollten als Input existierende Schutzprofile verwendet werden und eine Methode verwendet werden, die zur systemantischen Entwicklung von Schutzrprofilen aus rechtlichen Vorgaben vorgestellt wur-

de [SDNK+13]. In dieser Arbeit berichten wid über die unterschiedlichen Quellen und die Erfahrung bei der Erstellung eines Schutzprofils.

2 Related Work: Existierende Schutzprofile

Es existieren bereits eine Reihe von Common Criteria (CC) Schutzprofilen im Kontext von "elektronischen Wahlen", die wir als Grundlage nehmen. Diese werden im Folgenden vorgestellt:

Schutzprofil: Digitales Wahlstift-System (BSI-PP-0031). Das Schutzprofil [Bun07] zielt insbesondere auf den Einsatz *Digitalen Wahlstift-Systems* [AMBS07] für politische Wahlen ab. Der Evaluierungsgegenstand besteht aus folgenden Komponenten: 1) Der "Digitale Wahlstift" und die zugehörige "Dockingstation", 2) Firmware zur Aufzeichnung der Stimme, 3) Datenbank zur Speicherung der elektronischen Stimmen (elektronische Urne) und 4) Software zur Kontrolle der Abläufe der Wahlhandlung, Bewertung, Auszählung und Feststellung des Ergebnisses. Das Schutzprofil entspricht den Vorgaben der CC-Standard Version 2.3 und schlägt die Vertrauenswürdigkeitsstufe EAL3+ vor.

Schutzprofil: Basissatz von Sicherheitsanforderungen an Online-Wahlprodukte (BSI-PP-0037). Dieses Schutzprofil [Bun08a] definiert die Sicherheitsanforderungen, welche von Online-Wahlsysteme erfüllt werden müssen. Der Evaluierungsgegenstand ist ein verteiltes Client-Server-System, welches aus folgenden Komponenten besteht: 1) Dienstnutzer (Client), d.h. die Anwendersoftware des Wählers und 2) Dienstleister (Server), d.h. die Serversoftware. Die client-seitige Komponente ermöglicht den Wählern ihre Stimme online abzugeben. Die server-seitige Komponente verwaltet die Wahlberechtigungsliste und die Urne. Das Schutzprofil entspricht den Vorgaben der CC-Standard Version 3.1 Revision 2 und schlägt die Vertrauenswürdigkeitsstufe EAL2+ vor.

Schutzprofil: IEEE P1583. Das "IEEE P1583" Schutzprofil definiert die minimalen Sicherheitsanforderungen, die elektronische Wahlgeräte umsetzen müssen, um mit den Richtlinien 2002 FEC (Federal Election Commission Guidelines) und HAVA (Help America Vote Act) konform zu sein. Bei diesem Schutzprofil wurde keine Methodik zur Herleitung technischer Anforderungen aus den spezifischen rechtlichen Anforderungen verwendet. Der Evaluierungsgegenstand besteht aus der Software und Hardware des Wahlgeräts. Das Schutzprofil entspricht den Vorgaben der CC-Standard Version 2.3 und schlägt die Vertrauenswürdigkeitsstufe EAL2 vor.

Schutzprofil: PP-CIVIS. Ähnlich zu dem vorherigen Schutzprofil definiert das CIVIS-Schutzprofil [Sec06] von Wahlgeräten zu erfüllende Sicherheitsanforderungen. Der Evaluierungsgegenstand ist ebenfalls die Software und Hardware des Wahlgeräts. Das Schutz-

profil entspricht den Vorgaben der CC-Standard Version 3.0 und schlägt die Vertrauenswürdigkeitsstufe EAL2+ vor.

Schutzprofil: Kontrollierte elektronische Wahlgeräte. Dieses Schutzprofil [KKY12] definiert Sicherheitsanforderungen, die von Wahlgeräten erfüllt werden sollten. In diesem Schutzprofil wird die Bedeutung der Verifizierbarkeit hervorgehoben, aber ähnlich zu allen vorherigen Schutzprofilen werden keine Anforderungen bezüglich Verifizierbarkeit definiert. Der Evaluierungsgegenstand wird nicht genau spezifiziert. Das Schutzprofil entspricht den Vorgaben der CC-Standard Version 3.1 und schlägt die Vertrauenswürdigkeitsstufe EAL3+ vor.

Schutzprofil: Sichere elektronische Wahlgeräte. Im Gegensatz zu den IEEE P1583 und PP-CIVIS Schutzprofilen behandelt dieses Schutzprofil [LLWK10] Kiosk-Wahlgeräte. Kiosk-Wahlgeräte sind über ein Netzwerk verbundene Wahlgeräte, über die Wähler am Wahltag ihre Stimme an öffentlichen Plätzen abgeben können. Die Besonderheit dieses Schutzprofiles besteht darin, dass es das einzige Schutzprofil ist, welches Verifizierbarkeit einbezieht und es als Sicherheitsziel des Evaluierungsgegenstandes definiert. Der Evaluierungsgegenstand besteht aus der Software und Hardware des Wahlgeräts. Das Schutzprofil entspricht den Vorgaben des CC-Standard Version 3.1 und schlägt die Vertrauenswürdigkeitsstufe EAL4+ vor.

Vergleich existierende Schutzprofile. Tabelle 1 stellt einen Vergleich aller existierenden Schutzprofile, die für elektronische Wahlgeräte entworfen wurden, dar. Der Vergleich zeigt, dass alle Schutzprofile außer "Sichere elektronische Wahlgeräte" Verifizierbarkeit nicht einbeziehen und somit nicht mit dem Prinzip der *Öffentlichkeit der Wahl* konform sind. Wie bereits von Buchmann et al. [BNV14] festgestellt wurde, deckt jedoch das Schutzprofil "Sichere elektronische Wahlgeräte" Verifizierbarkeit nicht adäquat ab: Einerseits wird Verifizierbarkeit als Sicherheitsziel des Evaluierungsgegenstandes definiert, jedoch wird keine Beziehung (rationale) zwischen Sicherheitszielen und Sicherheitsanforderungen angegeben. Andererseits führt die Erweiterung der Sicherheitsanforderungen zu einem Schutzprofil, das außerhalb des CC-Standards. Letztlich werden die Sicherheitsanforderungen nicht systematisch aus rechtlichen Anforderungen heraus abgeleitet, was die Rechtskonformität der danach evaluierten Produkte in Frage stellt.

Verifizierbarkeit und Common Criteria In diesem Zusammenhang ist auch die Diskussion von Buchmann et al. [BNV14] zum Thema Schutzprofilen im Kontext von elektronischen Wahlen von Interesse. Einerseits wird dort festgestellt, dass es der Common Criteria an Flexibilität fehlt, den gesetzlichen Gestaltungsspielraum [NKH+13] umzusetzen. Andererseits wird festgestellt, dass die Berücksichtigung der Verifizierbarkeit in Schutzprofilen als besondere Herausforderung gilt, da entsprechende CC Komponenten nicht vorhanden sind. Gemäß ihrer Erkenntnisse, schlagen Buchmann et al. vor, auf Annahmen an die Vertrauenswürdigkeit des Wahlsystems zu verzichten, um die Verifizierbarkeit so implizit in das Schutzprofil zu integrieren.

Schutzprofil	Version	EAL	EVG	Verifizierbarkeit
BSI-PP-0031	2.3	3+	Docking Station Firmware, E-Urne, Software	Nein
BSI-PP-0037	3.1	2+	Client Server	Nein
IEEE P1583	2.3	2	Software, Hardware	Nein
PP-CIVIS	3.0	2+	Software, Hardware	Nein
Kontrollierte ele. Wahlgeräte	3.1	3+	-	Nein
Sichere ele. Wahlgeräte	3.1	4+	Software, Hardware	Ja

Tabelle 1: Vergleich existierender Schutzprofile.

3 Methode zur Entwicklung von Schutzprofilen

Dieser Abschnitt widmet sich den von Simić-Draws et al. [SDNK+13] vorgeschlagenen Schnittstellen zwischen den Methodiken und Standards *Konkretisierung Rechtlicher Anforderungen* (KORA) [Roß08], *Common Criteria* (CC) [Int09] und *IT-Grundschutz* [Bun08b] Standard. Die Schnittestellen erlauben u.a. Schutzprofile auf Basis rechtlicher Vorgaben zu entwickeln. Entsprechend ist die Idee, diesen Ansatz zu verwenden, um ein Schutzprofil für elektronische Wahlgeräte mit Paper Audit Trails zu entwickeln. Zunächst werden die einzelnen Methodiken und Standards beschrieben, dann die Schnittstellen.

KORA - Konkretisierung Rechtlicher Anforderungen Die Methodik *Konkretisierung Rechtlicher Anforderungen* (KORA) wurde von der *Projektgruppe verfassungsverträgliche Technikgestaltung* (provet) an der Universität Kassel entwickelt. Ziel der Methodik ist die Entwicklung technischer Konzepte juristisch zu begleiten und somit die Verfassungsverträglichkeit der Technik zu sichern. KORA sieht dazu folgenden Prozess vor: Nachdem man die rechtlichen Vorgaben, die für die neue Technik relevant sind, identifiziert hat, werden folgende Schritte ausgeführt: 1) *Konkretisierung rechtlicher Anforderungen*: Risiken und Chancen werden beschrieben, welche durch den Einsatz der Technik einen Einfluss auf die rechtlichen Vorgaben haben; 2) *Konkretisierung rechtlicher Kriterien*: Einzelne Aspekte der Anforderungen werden betont, welche die Technik erfüllen soll; 3) *Ableitung technischer Ziele*: Funktionen werden beschrieben, die den rechtlichen Kriterien entsprechen sollen. Hier findet ein Übergang von der juristischen in die technische Sprache statt; 4) *Ableitung technischer Gestaltungsvorschläge*: Konkrete technische Gestaltungsvorschläge werden aus den technischen Zielen abgeleitet.

CC - Common Criteria Der Common Criteria (CC)-Standard wurde entwickelt, um Produkte der Informationssicherheit zu evaluieren. Der CC-Standard umfasst zwei wesentliche Grundkonzepte: Schutzprofile und Security Targets. Der Fokus dieser Arbeit liegt auf Schutzprofilen, welche im Gegensatz zu Security Targets allgemein und unabhängig von einem konkreten Produkt definiert werden. Ein Schutzprofil besteht aus folgenden Teilen: 1) Definition des Sicherheitsproblems, 2) Sicherheitsziele, 3) funktionale Sicherheitsanforderungen und Vertrauenswürdigkeitsanforderungen an das Produkt (die spezifische Technik). Alle Anforderungen werden in zwei Katalogen bereitgestellt: 1) Komponenten der funktionalen Sicherheit; 2) Komponenten der vertrauenswürdigen Sicherheit. Diese Komponenten werden weiter in Klassen und Familien unterteilt, welche zur Überführung und Konkretisierung von Sicherheitszielen in Anforderungen verwendet werden. Durch die Bereitstellung von Anforderungskatalogen ist ein einheitliches Vokabular und somit die Vergleichbarkeit von Produkten gegeben. Schutzprofile werden darüber hinaus mit einer Vertrauenswürdigkeitsstufe (*engl.*: Evaluation Assurance Level (EAL)) versehen, die eine Prüftiefe für das Produkt gegen das Schutzprofil vorgibt. So kann die Prüftiefe zwischen EAL 1 (funktionell getestet) und EAL 7 (formal verifizierter Entwurf und getestet) liegen.

IT-Grundschutz Der IT-Grundschutz wurde vom Bundesamt für Sicherheit in der Informationstechnik (BSI) entwickelt. Ziel des IT Grundschutzes ist es eine einfache Methode bereit zu stellen, die Sicherheitsmaßnahmen mit einer an die Bedürfnisse angepassten Sicherheitsstufe für Standard-Schutzanforderungen zum Schutz von Geschäftsprozessen, Anwendungen und IT-Systemen liefert. Dazu werden organisatorische, personelle, infrastrukturelle und technische Maßnahmen vorgeschlagen. Der IT-Grundschutz besteht auf folgenden Katalogen: Bausteinen, Gefährdungen und Schutzmaßnahmen. Der Bausteine-Katalog ist in fünf Stufen unterteilt, nach denen sich Verantwortlichkeiten trennen lassen. Diese Stufen sind: Übergreifende Aspekte, Infrastruktur, IT-Systeme, Netze, Anwendungen. Für jeden konkreten Baustein (z.B. B 5.21 Webanwendungen) werden konkrete Gefährdungen aus dem Schichtenmodell des Gefährdungskatalogs identifiziert, sowie entsprechende Schutzmaßnahmen aus dem Schichtenmodell des Schutzmaßnahmenkatalogs genannt, die einen Grundschutz liefern.

Schnittstellen zwischen KORA, CC und IT-Grundschutz Simić-Draws et al. [SDNK+13] identifizieren Schwachstellen der jeweiligen Methodiken und Standards. So bietet KORA zwar eine rechtlich fundierte Grundlage zur Ableitung technischer Anforderungen, jedoch genügt diese Ableitung nicht zur vollständigen Evaluation von IT-Systemen. Während die Common Criteria ein etablierter IT Evaluationsstandard ist, werden rechtliche Anforderungen nicht betrachtet und eine rechtskonforme Evaluation von Produkten kann nicht ohne weiteres stattfinden. Schließlich bietet der IT-Grundschutz eine umfassende Sicherheitssicht, während auch der IT-Grundschutz einerseits rechtliche Aspekte nicht betrachtet, andererseits eine Produktevaluation nicht auf dem Detailgrad der Common Criteria stattfindet. Auf Grundlage dieser Erkenntnis erarbeiten Simić-Draws et al. eine Methodik, die die Schwachstellen der einzelnen Methodiken und Standards durch eine geeignete Komposition eliminiert. Diese Komposition ist in Abbildung 1 dargestellt.

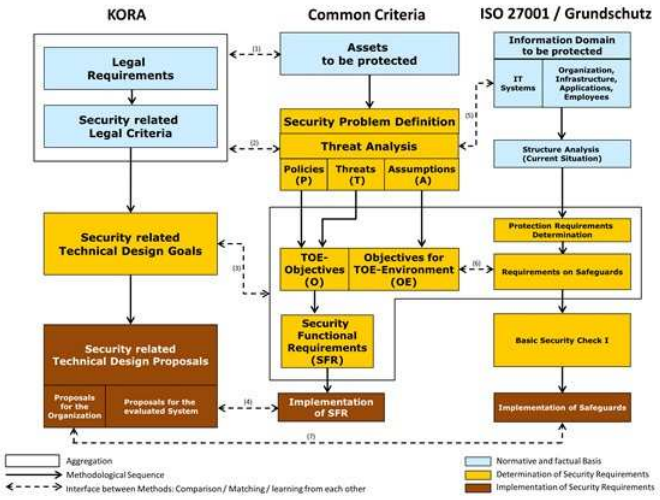

Abbildung 1: Schnittstellen zwischen KORA, CC und IT-Grundschutz [SDNK+13].

4 Operationalisierung der Methode

Bei dem Versuch, die Methode anzuwenden, hat sich gezeigt, dass weitere Konkretisierungen notwendig sind, um diese in Bezug auf die Entwicklung von Schutzprofilen operationalisieren zu können. Die im Rahmen dieser Arbeit vorgeschlagenen Konkretisierungen sind in Abbildung 2 fett umrandet.

Im Vordergrund stehen dabei zunächst die zu schützenden Werte, die als Basis für alle weiteren Schritte bei der Entwicklung eines Schutzprofils dienen. Wir schlagen vor, die zu schützenden Werte wie folgt aus den mittels KORA ermittelten rechtlichen Kriterien abzuleiten: In einem ersten Schritt werden die Kriterien semantisch analysiert und in Teilkriterien unterteilt. In einem zweiten Schritt sollen in einem interdisziplinären Diskurs zwischen juristischen und technischen Experten die sicherheitsrelevanten Teilkriterien identifiziert werden. Im nächsten Schritt können dann auf Basis der sicherheitsrelevanten Teilkriterien die zu schützenden Werte identifiziert werden.

Die Grundlage für die Beschreibung der Einsatzumgebung (Bedrohungen, Annahmen und Sicherheitspolitiken) bildet klassich eine Bedrohungsanalyse. Um diese auf die zuvor identfizierten zu schützenden Werte anwenden zu können, wird folgender Prozess vorgeschlagen: Basierend auf den kryptographischen Schutzzielen Authentizität, Integrität und Vertraulichkeit soll im interdiziplinären Dialog geklärt werden, welches die relevanten Schutzziele für den jeweiligen zu schützenden Wert sind. Die Bedrohungsanalyse kann dann anhand von Bedrohungsbäumen durchgeführt werden.

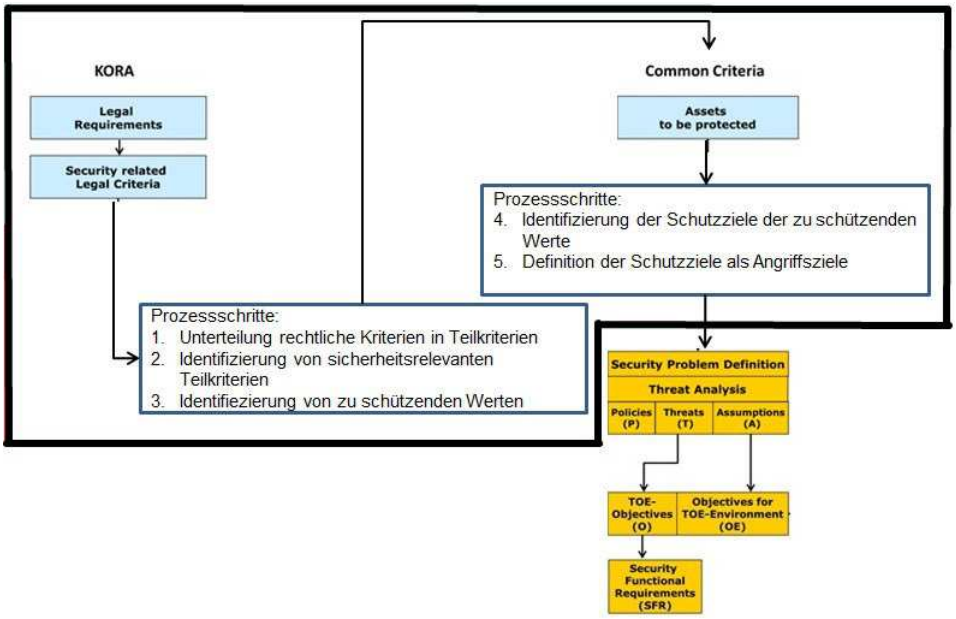

Abbildung 2: Fokus und Verfeinerung der Evaluationsmethodik [SDNK+13].

5 Entwurf des Schutzprofils

Aufgrund der Tatsache, dass ein vollständiges Schutzprofil den Rahmen dieser Arbeit sprengen würde, beschränken wir uns an dieser Stelle auf folgende Bestandteile des Schutzprofils: 1) Beschreibung des Evaluierungsgegenstands 2) Liste der zu schützenden Werte (an ausgewählten Beispielen), 3) Bedrohungsgraph für die zu schützenden Werte als Basis für die Definition der Einsatzumgebung.

5.1 Der Evaluierungsgegenstand

Der betrachtete Evaluierungsgegenstand (EVG) ist ein elektronisches Wahlsystem, das die Kandidatenauswahl an einem elektronischen Wahlgerät sowie die Auszählung an einem anderen elektronischen Wahlgerät vorsieht. Der EVG besteht aus einem hybriden Wahlgerät. Ähnlich zur papier-basierten Wahl identifiziert sich der Wähler zunächst gegenüber dem Wahlvorstand. Danach betritt er die Wahlkabine und benutzt das elektronische Wahlgerät um durch das Auswählen der Kandidaten seinen Stimmzettel zu erstellen. Sobald der Wähler seine Auswahl bestätigt wird der Stimmzettel ausgedruckt. Der ausgedruckte Stimmzettel enthält einen menschlich- und einen maschinen-lesbaren Teil. Beide Teile ent-

halten dieselbe Information, nämlich die Auswahl des Wählers.[1] Der menschlich-lesbare Teil dient dem Wähler zur Überprüfung, dass der gedruckte Stimmzettel der am Wahlgerät abgegebenen Stimme entspricht. Nach der Überprüfung durch den Wähler faltet dieser den Stimmzettel, verlässt die Wahlkabine und wirft den Stimmzettel in die Wahlurne. Der maschinen-lesbare Teil des Stimmzettels ermöglicht ein automatisiertes Auszählen der gedruckten Stimmzettel. Es gibt bereits einige Wahlsysteme (Wahlgeräte), welche diesem Evaluierungsgegenstand entsprechen, zum Beispiel [BNFL+12], [VBD11], [Veg12], and [Vot11].

Die Komponenten des Evaluierungsgegenstand sind in Abbildung 3 dargestellt. Der Evaluierungsgegenstand beinhaltet die Hardware und Software dieser Komponenten.

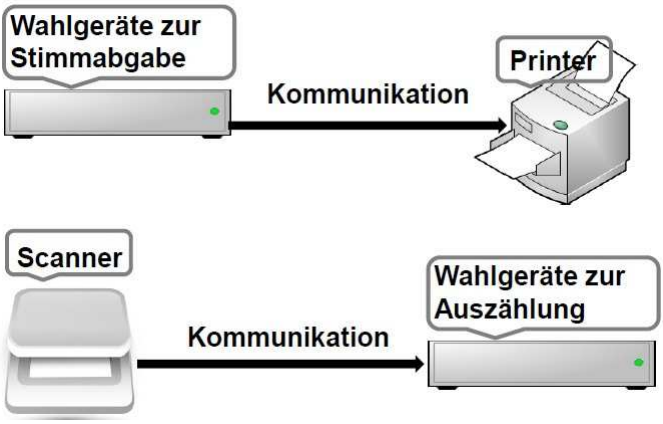

Abbildung 3: Komponentente des Evaluierungsgegenstandes.

5.2 Identifizierung der zu schützenden Werte

In diesem Abschnitt wenden wir die in dieser Arbeit eingeführte Verfeinerung der Evaluationsmethodik von Simić-Draws et al. [SDNK+13] an und führen die Identifizierung von zu schützenden Werten beispielhaft durch. Als Beispiel verwenden wir das rechtliche Kriterium der Manipulationssicherheit. Dieses Kriterium steht indirekt im Bezug zur Verifizierbarkeit, weil es voraussetzt, dass Manipulationen nicht unentdeckt bleiben können, d.h. es fordert einen Mechanismus zur Verifikation.

Aus dem rechtlichen Kriterium der Manipulationssicherheit[2], werden folgende sicherheitsrelevante Teilkriterien abgeleitet:

1. Eine Manipulation von amtlich zugelassenen und genehmigten Geräten darf nicht

[1] Im Falle einer Abweichung zwischen dem menschlich- und dem maschinen-lesbaren Teil, zählt ausschließlich der menschlich-lesbare Teil des Stimmzettels.

[2] Die vollständige Definition dieses rechtliche Kriterium befindet sich in [Hen14].

unentdeckt bleiben.

2. Eine nachträgliche Änderung der Software bzw. Hardware des EVGs muss unmöglich sein oder darf zumindest nicht unentdeckt bleiben.

5.3 Identifizierung von Bedrohungen

Die beiden zuvor identifizierten sicherheitsrelevanten Teilkriterien sind über den zu schützenden Wert *Geräte* verbunden. Das einzige relevante Schutzziel dieses zu schützenden Wertes ist die Integrität und das daraus entstehende Angriffsziel ist *Verletzung der Integrität der Geräte*. Der Bedrohungsbaum zu diesem Angriffsziel ist in Abbildung 4 dargestellt. Einige der möglichen Bedrohungen, welche in diesem Bedrohungsbaum identifiziert wurden, wurden aus vorherigen Arbeiten entnommen, siehe Prosser et al. [PKKU04] and Krimmer and Volkamer [KV08].

Aus den Blättern dieses Bedrohungsbaumes können die entsprechenden *Bedrohungen* und *Annahmen* identifiziert werden. In Anlehnung an Buchmann et al. [BNV14] kann nur eine Kombination an zulässigen Bedrohungen und Annahmen in einem Schutzprofil abgebildet werden, nicht aber alle laut Gestaltungsspielraum möglichen. Welche Kombination gewählt wird, sollte im interdisziplinären Dialog entschieden werden.

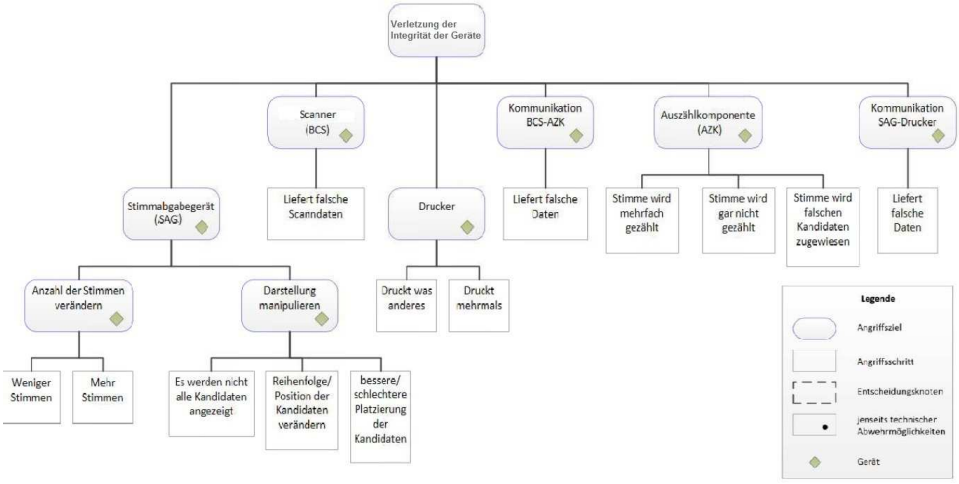

Abbildung 4: Bedrohungsbaum “Manipulierte Geräte”.

6 Zusammenfassung

Mit dem stetigen Fortschreiten der Entwicklung, dringen Technologien in immer neue Bereiche unseres Lebens vor. War die Durchführung von Wahlen über Jahrhunderte ein relativ simpler Prozess, so eröffnen elektronische Wahlsysteme neue Möglichkeiten zur Schaffung und Festigung von Demokratien. Obwohl elektronische Wahlen in Deutschland bereits praktisch durchgeführt wurden, hat das Bundesverfassungsgericht mit dem Urteil vom 3. März 2009 die Durchführung bisheriger elektronischer Wahlen für verfassungswidrig erklärt. Grund dieses Urteils war die Tatsache, dass die eingesetzten Wahlgeräte nicht dem Prinzip der *Öffentlichkeit der Wahl* entsprachen. Die Durchführung rechtskonformer elektronischer Wahlen ist eine Herausforderung von besonderem öffentlichen Interesse und bedarf interdisziplinärer Forschungsarbeit. Ziel dieser Arbeit war es einen ersten Schritt in Richtung Entwurf eines Schutzprofils zur Evaluierung von elektronischen Wahlgeräten mit Paper Audit Trails auf Basis rechtlicher Vorgaben zu entwickeln. Dazu wurde in dieser Arbeit eine der Schnittstellen zwischen KORA und dem CC-Standard der Evaluationsmethodik nach Simić-Draws et al. [SDNK+13] bezüglich einer systematischen Methodik zur Identifizierung von zu schützenden Werten verfeinert.

Danksagung

Wir danken den anonymen Gutachtern mit deren Hilfe die Qualität dieser Arbeit deutlich verbessert werden konnte. Diese Arbeit wurde im Rahmen des durch die DFG geförderten Projektes 'VerkonWa' - Verfassungskonforme Umsetzung von elektronischen Wahlen sowie durch das vom Center for Advanced Security Research Darmstadt (CASED) geförderte Projekt ComVote entwickelt.

Literatur

[AMBS07] J. Arzt-Mergemeier, W. Beiss und T. Steffens. The Digital Voting Pen at the Hamburg Elections 2008: Electronic Voting Closest to Conventional Voting. In A. Alkassar und M. Volkamer, Hrsg., *E-Voting and Identity*, Jgg. 4896 of *Lecture Notes in Computer Science*, Seiten 88–98. Springer Berlin Heidelberg, 2007.

[BNFL+12] J. Ben-Nun, N. Fahri, M. Llewellyn, B. Riva, A. Rosen, A. Ta-Shma und D. Wikström. A New Implementation of a Dual (Paper and Cryptographic) Voting System. In *Electronic Voting*, Jgg. 205 of *LNI*, Seiten 315–329, 2012.

[BNV14] J. Buchmann, S. Neumann und M. Volkamer. Tauglichkeit von Common Criteria-Schutzprofilen für Internetwahlen in Deutschland. *Datenschutz und Datensicherheit - DuD*, 38(2):98–102, 2014.

[Bun07] Bundesamt für Sicherheit in der Informationstechnik. Schutzprofil Digitales Wahlstift-System (Version 1.0.1), März 2007.

[Bun08a] Bundesamt für Sicherheit in der Informationstechnik. Basissatz von Sicherheitsanforderungen an Online-Wahlprodukte (Version 1.0), April 2008. https://www.commoncriteriaportal.org/files/ppfiles/pp0037b.pdf.

[Bun08b] Bundesamt für Sicherheit in der Informationstechnik. IT-Grundschutz Methodology, BSI Standard 100-2 (Version 2.0), May 2008.

[Bun09] Bundesverfassungsgerichts. Entscheidungen des Bundesverfassungsgerichts. BVerfGE 123, 39 - 81, March 2009. http://www.bverfg.de/entscheidungen/cs20090303$_2bvc$000307.$html$.

[Hen14] M. Henning. Transparenz und Sicherheit in der Demokratie - Verfassungsverträglichkeit elektronischer Wahlgeräte. Diss., Universität Kassel, 2014.

[HVB12] M. Henning, M. Volkamer und J. Budurushi. Elektronische Kandidatenauswahl und automatisierte Stimmermittlung am Beispiel hessischer Kommunalwahlen. *Die Öffentliche Verwaltung (DÖV)*, (20), October 2012.

[Int09] International Organization for Standardization. ISO/IEC 15408: Common Criteria for Information Technology Security Evaluation, Part 1–3 (Version 3.1, Revision 3), July 2009.

[KKY12] G. R. Karokola, S. Kowalski und L. Yngström. Secure e-Government services: Protection Profile for Electronic Voting - A Case of Tanzania. In *IST-Africa 2012 Conference Proceedings*, 2012.

[KV08] R. Krimmer und M. Volkamer. Observing Threats to Voter's Anonymity: Election Observatio of Electronic Voting. In S. J. Krishna und N. K. Agarwal, Hrsg., *E-Voting - Perspectives and Experiences*, The Icfai University Press, 2008.

[LLWK10] K. Lee, Y. Lee, D. Won und S. Kim. Protection Profile for Secure E-Voting Systems. In J. Kwak, R. Deng, Y. Won und G. Wang, Hrsg., *Information Security, Practice and Experience*, Jgg. 6047 of *Lecture Notes in Computer Science*, Seiten 386–397. Springer Berlin Heidelberg, 2010.

[NKH+13] Stephan Neumann, Anna Kahlert, Maria Henning, Philipp Richter, Hugo Jonker und Melanie Volkamer. Modeling the German Legal Latitude Principles. In *Electronic Participation*, Seiten 49–56. Springer, 2013.

[PKKU04] A. Prosser, R. Kofler, R. Krimmer und M. K. Unger. Security assets in e-voting. In *The International Workshop on Electronic Voting in Europe*, 2004.

[Roß08] A. Roßnagel. Rechtswissenschaftliche Gestaltung von Informationstechnik. In H. Kortzfleisch und O. Bohl, Hrsg., *Wissen, Vernetzung, Virtualisierung*, Seiten 381–390. Köln, Germany: Josef Eul Verlag, 2008.

[SDNK+13] D. Simić-Draws, S. Neumann, A. Kahlert, P. Richter, R. Grimm, M. Volkamer und A. Roßnagel. Holistic and Law compatible IT Security Evaluation: Integration of Common Criteria, ISO 27001/IT-Grundschutz and KORA. *International Journal of Information Security and Privacy (IJISP)*, 7(3):16–35, 2013.

[Sec06] Secretariat general de la defense nationale. Protection Profile: Machine a voter, PP-CIVIS (Version 1.0), Juni 2006. https://www.commoncriteriaportal.org/files/ppfiles/pp0037b.pdf.

[VBD11] M. Volkamer, J. Budurushi und D. Demirel. Vote casting device with VV-SV-PAT for elections with complicated ballot papers. In *International Workshop on Requirements Engineering for Electronic Voting Systems (REVOTE'11)*, Seiten 1–8. IEEE, August 2011.

[Veg12] C. Vegas. The New Belgian E-voting System. In *Electronic Voting*, Jgg. 205 of *LNI*, Seiten 199–211, 2012.

[Vot11] 2011. Vot.ar, http://www.vot-ar.com.ar/en/system-votation/.