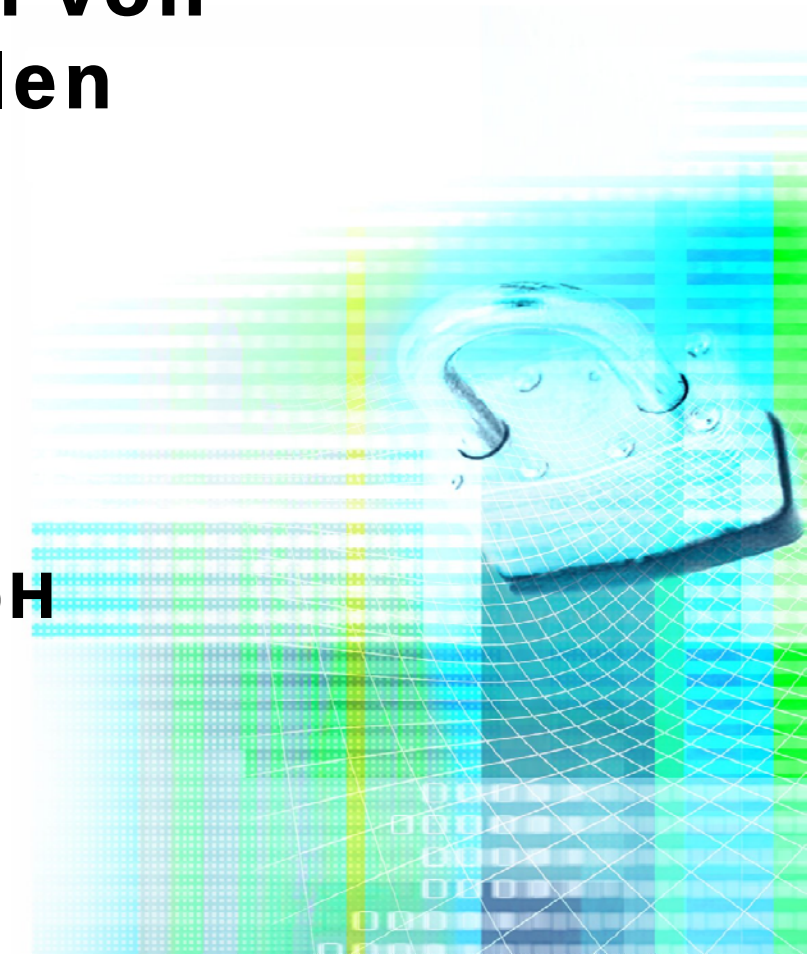
Chancen und Risiken von elektronischen Wahlen

Dr. Christian Paulsen

DFN-CERT Services GmbH

paulsen@dfn-cert.de



Agenda

- **Einführung**
- **Vorgehensweise Dissertation**
- **Bedrohungsanalyse**
- **Analyse existierender Wahlverfahren**
- **Anwendungskontexte**
- **Ergebnisse / Zusammenfassung**

Einführung

- **Definition Elektronische Wahlen**
  - Verwendung elektronischer Hilfsmittel bei der Durchführung mindestens einer der folgenden Prozesse:
    - Wähleridentifizierung
    - Stimmabgabe
    - Stimmauszählung

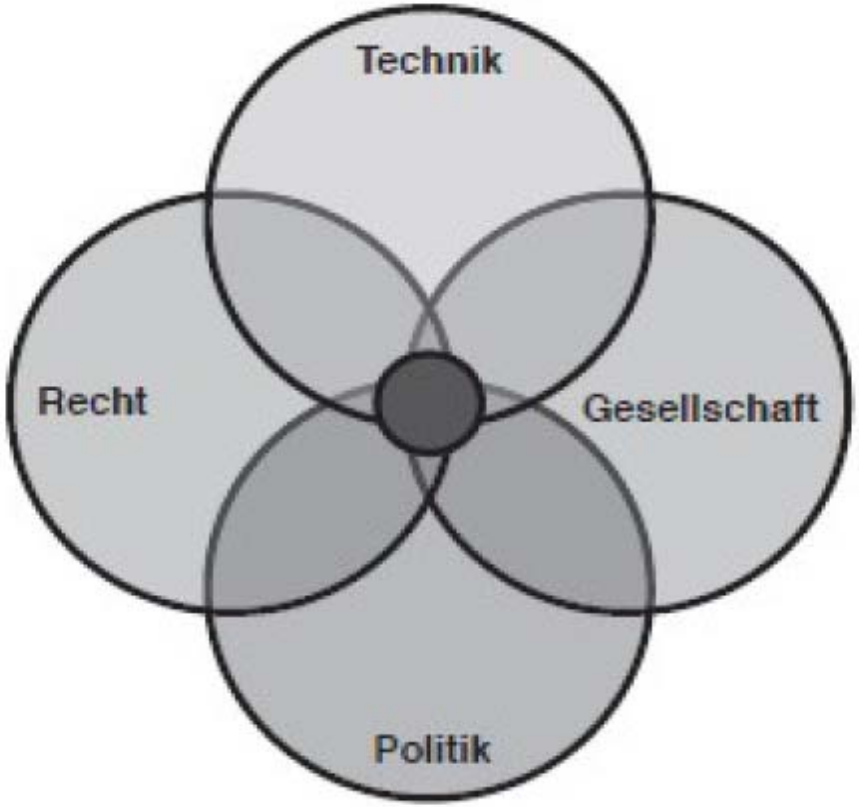
Einführung: Warum E-Voting?

- Schnelle und automatisierte Ergebnisermittlung
- Unterstützung der Wähler bei komplexen Wahlverfahren / Fehlerkorrekturen
- Ortsunabhängige Stimmabgabe
- Junge Wähler motivieren / Moderner Staat
- Erhöhung der Wahlbeteiligung
- Verifizierbarkeit
- Kosten

Einführung: Nachteile E-Voting

- Sicherheit / Manipulierbarkeit
- Komplexität
- Transparenz / Nachvollziehbarkeit eingeschränkt
- Rechtskonformität?
- „Junk Voting“
- „Family Voting“
- Digitale Spaltung
- Kosten

Einführung



Quelle: B. von Prollius: Rechtliche und technische Aspekte von Internetwahlen im internationalen Kontext, Hochschule der Medien Stuttgart, 2008

Einführung

- **Varianten elektronischer Wahlverfahren:**
  - Stand-Alone-Verfahren
    - Wahlgeräte / Wahlcomputer
    - Digitaler Wahlstift
  - Mobile Voting
    - Wahlen per SMS
  - Internetwahlverfahren
    - Wahlen via Internet
  - Mischformen:
    - Vernetzte Wahlgeräte / Smartphones u. Laptops

Einführung

	Präsenzwahlen	Distanzwahlen
Elektronische Wahlen	Wahlcomputer / Digitaler Wahlstift	Internetwahlen
Papierbasierte Wahlen	Wahlen im Wahllokal mit Wahlurne	Briefwahlen

Einführung: Wahlgeräte

- **Beispiel NEDAP-Geräte:**
  - Bedieneinheit für den Wahlvorstand
  - Programmier- und Ausleseeinheit
  - Serielle Verbindung mit PC, auf dem die Wahlsoftware läuft
  - Viele Angriffsmöglichkeiten:
    - Austausch / Umprogrammieren des internen Speichermoduls
    - Wahlsoftware manipulieren
    - Sämtliche Schnittstellen angreifbar (Innentäter)
    - Sicherheitsprinzip: „Security by Obscurity“

Einführung: Wahlgeräte

Quelle: Chaos Computer Club

Einführung: Wahlgeräte

- Mehrfacher Einsatz bei parlamentarischen Wahlen
- Viele Proteste (Deutschland, Niederlande, Irland...)
- Bundesverfassungsgericht: Einsatz von NEDAP-Wahlgeräten bei Bundestagswahl 2005 verfassungswidrig
- Hauptkritikpunkt: Mangelnde Nachvollziehbarkeit / Überprüfbarkeit

Einführung: Wahlgeräte

- **Digitaler Wahlstift**
  - Geplanter Einsatz bei der Hamburger Bürgerschaftswahl 2008
  - Grund: Komplexes Wahlverfahren
  - Expertenrunde äußerte Bedenken
  - Folgen: Wahlstift wurde nicht eingesetzt

Quelle: http://www.halbach.com

Einführung: Mobile Voting

- **Mobile Voting: Abstimmung per SMS**
  - Beispiel:

Vorlage	Identifikation	JA	NEIN
Vorlage 1	89876765	7873	2198
Vorlage 2	56438237	4362	3442

  - Zustimmung zur Gesetzesvorlage 1:
  - SMS mit dem Inhalt „89876765-7873“ an ein zentrales Stimmregister senden

Einführung: Mobile Voting

- 2005: Schweizer Kanton Zürich setzt M-Voting testweise bei Volksabstimmung ein
- Ergebnis: Nicht zukunftsträchtig, keinen weiteren Einsatz
- Bedrohungen:
  - Gefälschte SIM-Karten
  - IMSI (Int. Mobile Subscriber Identity)-Catcher als Man-In-The Middle Angriff
  - DOS-Attacken
  - Manipulation der Mobilfunkgeräte mittels Over-The-Air-Provisioning
  - Insiderattacken

Einführung: Internetwahlen

- **Wahlen via Internet**
- **Komplexeste E-Voting-Variante**
- **Wahlsystem bestehend aus:**
  - Wahlserver
  - Wahlclient
  - Wahlsoftware
- **Herausforderung: Trennung von Authentizität und Stimmabgabe**
- **Theoretische kryptographische Konzepte gibt es seit 1980**

Einführung: Internetwahlen

- **Bereits durchgeführte Internetwahlen (Beispiele):**
  - Studierendenwahl Uni Osnabrück 2000
  - Estland 2005 (Kommunalwahlen) und 2007 (Parlamentswahlen)
  - GI-Präsidiumswahlen seit 2006
  - Österreichische Hochschulwahlen 2009
  - Betriebsratswahlen Deutsche Telekom 2005
  - Umfangreiche E-Voting-Datenbank unter http://www.e-voting.cc

Einführung: Stand E-Voting

- **Diskussionen über das Pro und Contra von E-Voting**
  - Emotional geführte Lagerkämpfe
- **Fokus auf Sicherheitsfragen**
  - Vernachlässigung Praxisrelevanz / Benutzbarkeit
- **Fokus liegt auf politischen Präsenzwahlen**
  - Vernachlässigung anderer Anwendungskontexte
- **„NEDAP-Urteil“ des Bundesverfassungsg.**
  - Das Aus für E-Voting?

Agenda

- Einführung
- Vorgehensweise Dissertation
- Bedrohungsanalyse
- Analyse existierender Wahlverfahren
- Anwendungskontexte
- Ergebnisse / Zusammenfassung

Vorgehensweise

- **Beschränkung auf Internetwahlverfahren**
- **Erarbeiten der Anforderungen für Sicherheit und Praxisrelevanz**
- **Basis:**
  - Wahlrechtsgrundsätze
  - Bedrohungsanalyse

Vorgehensweise

- **Analyse existierender Wahlverfahren:**
  - Sicherheit
  - Praxisrelevanz und Benutzbarkeit
- **Unterschiedliche Anwendungsbereiche berücksichtigen**
  - Spezifische Anforderungen erarbeiten
- **Empfehlungskatalog erstellen**

Wahlrechtsgrundsätze

- **Wahlrechtsgrundsätze (GG, Artikel 38, Abs.1):**
  - Allgemein (Jeder darf wählen)
  - Frei (ohne Beeinflussung und Zwang)
  - Unmittelbar (Verteilung d. Sitze anhand der Wählerstimmen)
  - Geheim
  - Gleich (gleiche Rechte für Alle)
    - Öffentlich / transparent
- **Teilweise im Konflikt zueinander!**

Agenda

- Einführung
- Vorgehensweise Dissertation
- Bedrohungsanalyse
- Analyse existierender Wahlverfahren
- Anwendungskontexte
- Ergebnisse / Zusammenfassung

Bedrohungsanalyse

- **Bedrohungen Wahlclient:**
  - Malware
    - Viren, Trojaner, Würmer, Rootkits, Hoaxes...
  - Phishing
  - (Automatisierte) Netzwerkattacken
    - Ausnutzen von Softwareschwachstellen
    - Ausnutzen sonstiger Lücken (z.B. Default-Passwörter, ungeschützter Netzwerkzugang)
  - Hardwaredefekte / Funktionsstörungen

Bedrohungsanalyse

- **Bedrohungen Wahlserver:**
  - Malware
  - Netzwerkattacken
    - (Distributed) Denial-of-Service-Angriffe
  - Hardwaredefekte / Funktionsstörungen
  - Insiderangriffe

Bedrohungsanalyse

- **Bedrohungen Übertragungskanal:**
  - Man-in-the-middle-Angriffe:
    - DNS-Spoofing / IP-Spoofing
    - Mitlesen / Entschlüsseln von Stimmdaten
    - Manipulation von Stimmdaten
  - Verbindungsunterbrechung

Bedrohungsanalyse

- **Sonstige Bedrohungen**
  - Erpressung
  - Stimmenkauf
  - Menschliches Fehlverhalten
  - Fehler in der Wahlsoftware (absichtlich und fahrlässig)

Bedrohungsmatrix

Verursacher → / Schaden ↓	Externer Angreifer	Interner Angreifer	Probleme beim Betrieb des Wahlsystems
Angriff auf die **Integrität** des Wahlergebnisses	• Manipulation des Wahlservers / der Clientsoftware • Stimmenkauf • Wählen mit erschlichenen Zugangsdaten	• Manipulation der Stimmen oder der Clientsoftware • Wählen mit nicht genutzten Wählerkonten	• Systemfehler • Systemabstürze
Angriff auf die **Vertraulichkeit** der Stimmabgabe	• Man-in-the-middle-Attacken • Phishing	• Einbauen von Hintertüren zur Weiterleitung sensibler Daten	• Offenlegung, wer welche Stimme abgegeben hat
Angriff auf die **Verfügbarkeit** der Wahl	• (Distributed) Denial of Service Attacken	• Wahlserver abschalten	• Ausfall des Systems
Angriff auf die **Akzeptanz** des Wahlverfahrens	• Verbreiten von Hoaxes per Mail	• Verkünden, dass das System unsicher ist	• Schlechte Usability • zu komplexes Verfahren

Agenda

- Einführung
- Vorgehensweise Dissertation
- Bedrohungsanalyse
- Analyse existierender Wahlverfahren
- Anwendungskontexte
- Ergebnisse / Zusammenfassung

Analyse: Anforderungen

- **Sicherheitsanforderungen:**
  - **Vertraulichkeit** der Stimmabgabe
  - **Verfügbarkeit** des Wahlsystems
  - **Integrität** / Manipulationssicherheit
  - **Authentizität** aller beteiligten Instanzen
  - **Verhinderung von Stimmenkauf und Erpressbarkeit**
  - **Verifizierbarkeit** / Überprüfbarkeit

Analyse: Anforderungen

- **Anforderungen Praxisrelevanz und Benutzbarkeit:**
  - **Aktualität:** Entwicklungsstand (kein Prototyp, ausreichend getestet), Supportmöglichkeiten
  - **Transparenz:** verständlich und nachvollziehbar
  - **Kosten:** finanzieller und organisatorischer Aufwand (Vergleichsmaßstab: Briefwahlen)
  - **Usability:** ohne Spezialkenntnisse intuitiv benutzbar

Analyse: Kriterien

- **Vier Bewertungsstufen:**
  - Anforderung nicht erfüllt / keine Informationen (0)
  - Anforderung teilweise erfüllt (1)
  - Anforderung größtenteils erfüllt (2)
  - Anforderung erfüllt (3)

Analyse: Kriterien

- **Beispiel: Verifizierbarkeit**

	Individuell verifizierbar	Universell verifizierbar
Schwach verifizierbar	Der einzelne Wähler kann prüfen, ob seine Stimme überhaupt berücksichtigt wurde	Alle Wähler können den Wahlablauf prüfen und beobachten
Stark verifizierbar	Der Wähler kann zusätzlich prüfen, ob seine Stimmabgabe korrekt ins Ergebnis eingeflossen ist	Alle Wähler können zusätzlich prüfen, ob alle Stimmen von autorisierten Wählern abgegeben wurden

Analyse: Kriterien

- **Beispiel: Verifizierbarkeit**

- 0: Das Wahlergebnis ist nicht überprüfbar (Anf. nicht erf.)
- 1: Das Wahlergebnis ist schwach individuell oder schwach universell verifizierbar (Anforderung teilweise erfüllt)
- 2: Das Wahlergebnis ist stark individuell oder stark universell verifizierbar (Anforderung größtenteils erfüllt)
- 3: Das Wahlergebnis ist stark individuell und stark universell verifizierbar (Anforderung erfüllt)

Analyse: Darstellung

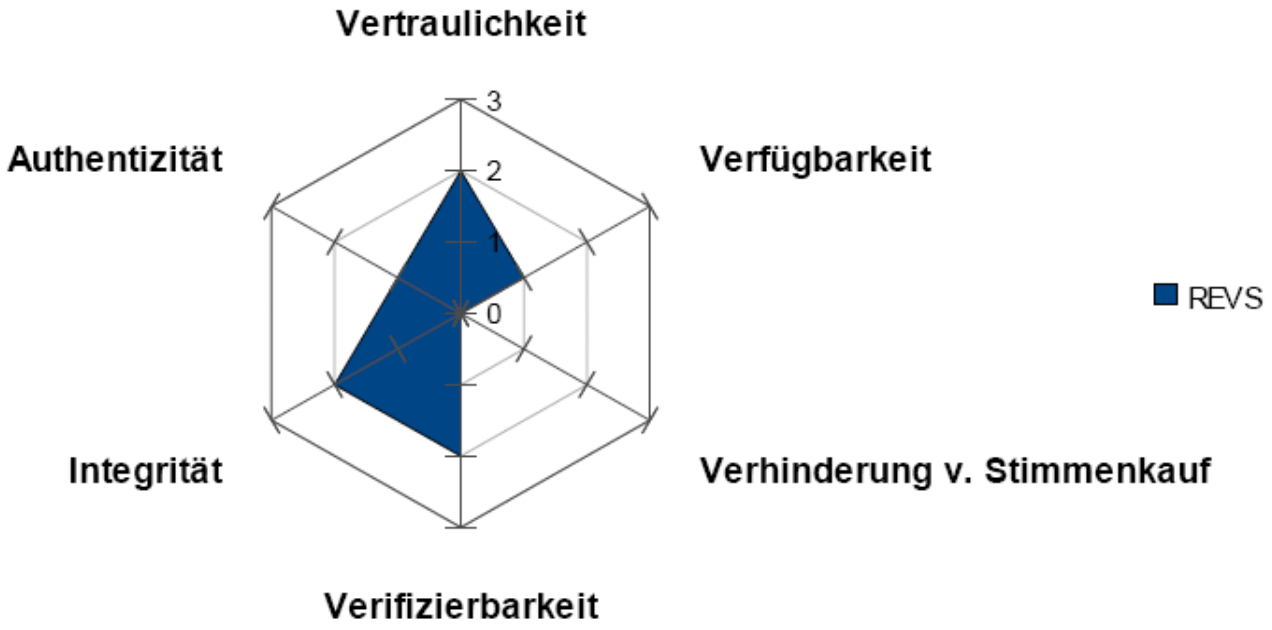


Abbildung 48: Ergebnis Sicherheitsanalyse REVS; C. Paulsen nach [Prosser et al., 2004]

Analyse: Verfahren

- **Evaluierte Wahlverfahren:**
  - POLYAS
  - EVOX
  - REVS
  - SERVE
  - Voteremote / W.I.E.N. / T-Vote
  - Adder
  - Helios
  - Pnyx
  - Estnisches Wahlsystem

Agenda

- Einführung
- Vorgehensweise Dissertation
- Bedrohungsanalyse
- Analyse existierender Wahlverfahren
- Anwendungskontexte
- Ergebnisse / Zusammenfassung

Anwendungskontexte

- **Anwendungsszenario A: Politische Wahlen**
  - A1: Präsenzwahl mit Papierstimmzetteln
  - A2: Briefwahlverfahren
- **Anwendungsszenario B: Wahlen im Wirtschaftsumfeld**
  - B1: Präsenzwahl mit Papierstimmzetteln
  - B2: Briefwahlverfahren
- **Anwendungsszenario C: Wahlen in nichtpolitischen Organisationen / Vereinen**
  - C1: Präsenzwahl mit Papierstimmzetteln
  - C2: Briefwahlverfahren
  - C3: Präsenzwahl mit Handabstimmung

Anwendungskontexte

- **Ersetzen / Ergänzen der existierenden Verfahren durch elektronisches Verfahren nur dann sinnvoll, wenn insgesamt *mindestens* das Niveau gehalten wird!**

- **Daher: Äquivalente Analyse nichtelektronischer Verfahren**

- **Ergebnisse dienen als Kriterium / Referenz für Eignungsanalyse**

- **Beispiel: Ergebnisse Parlamentarische Wahlen mit Papierstimmzetteln**

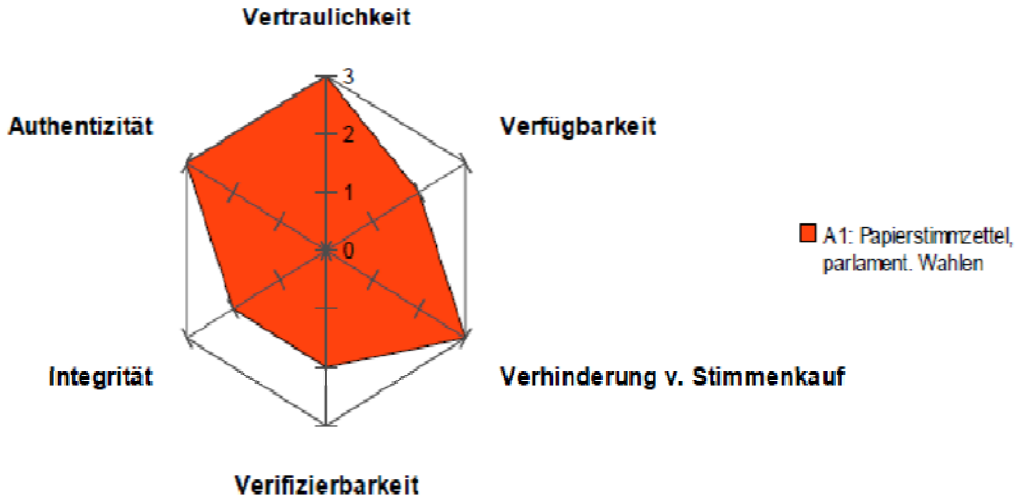


Abbildung 66: Szenario A1: Ergebnis Sicherheitsanalyse Präsenzwahlen mit Papierstimmzetteln bei parlamentarischen Wahlen; C. Paulsen nach [Prosser et al, 2004]

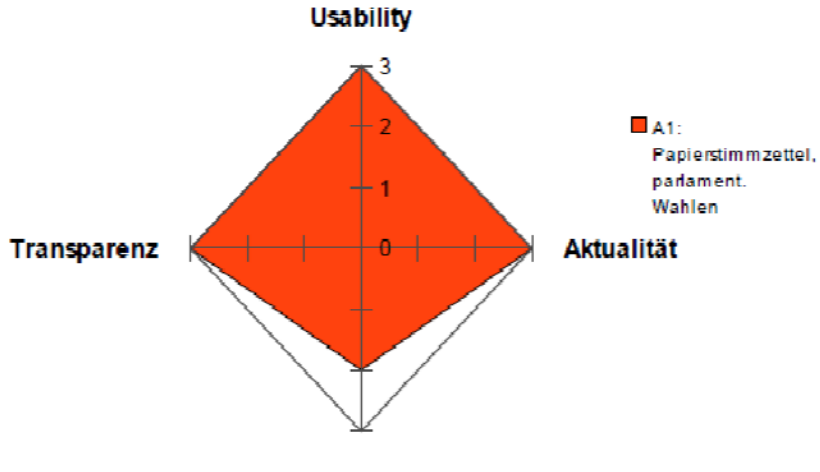
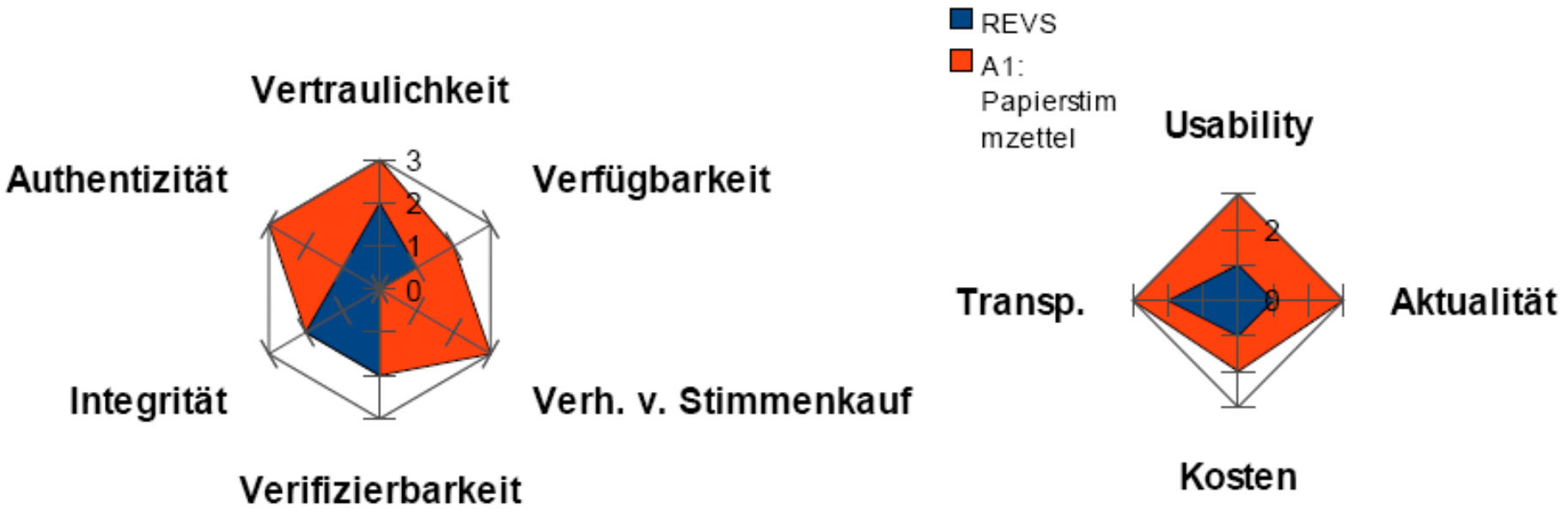


Abbildung 67: Szenario A1: Ergebnis Präsenzwahlen mit Papierstimmzetteln bei parlamentarischen Wahlen hinsichtlich Praxisrelevanz / Benutzbarkeit; C. Paulsen, nach [Prosser et al, 2004]

- **Überlagerung der Spiderwebdiagramme**



Ergebnis REVS: Nicht geeignet für Szenario A1

Agenda

- Einführung
- Vorgehensweise Dissertation
- Bedrohungsanalyse
- Analyse existierender Wahlverfahren
- Anwendungskontexte
- Ergebnisse / Zusammenfassung

Ergebnisse / Fazit

- **Für einen Ersatz nicht geeignete Verfahren:**
  - Erfüllen insgesamt die Anforderungen schlechter als nichtelektronische Verfahren
- **Bedingt geeignete Verfahren:**
  - Ausgeglichenes Verhältnis zwischen Mehrwert und Nachteil / Nachbesserungen möglich
- **Geeignetes Verfahren:**
  - Mehrwert ist vorhanden

Ergebnisse / Fazit

Verfahren	Ergebnis Sicherheit	Ergebnis Praxisrelevanz	Geeignet für	Bedingt geeignet für	Anmerkungen
SERVE	Authentizität: ■□□ Vertraulichkeit: ■□□ Integrität: ■□□ Verh. v. Stimmenkauf: □□□ Verifizierbarkeit: □□□ Verfügbarkeit: □□□	Aktualität: ■□□ Kosten: ■□□ Usability: ■□□ Transparenz: ■□□	- - -	- - -	- nach vernichtender Sicherheitsanalyse eines Expertengremiums in 2004 wurde SERVE nicht mehr eingesetzt
Voteremote (T-Vote / W I E N)	Authentizität: ■□□ Vertraulichkeit: ■■□ Integrität: ■■□ Verh. v. Stimmenkauf: ■□□ Verifizierbarkeit: ■□□ Verfügbarkeit: ■□□	Aktualität: ■■□ Kosten: ■□□ Usability: ■□□ Transparenz: ■□□	**C2: Briefwahlverfahren**	**A2: Briefwahlverfahren** **B2: Briefwahlverfahren** **C1: Präsenzwahl mit Papierstimmzetteln**	- Proprietäres Wahlverfahren - wird für Betriebsratswahlen der Telekom eingesetzt
Adder	Authentizität: ■□□ Vertraulichkeit: ■■□ Integrität: ■□□ Verh. v. Stimmenkauf: ■□□ Verifizierbarkeit: ■■□ Verfügbarkeit: □□□	Aktualität: ■□□ Kosten: ■□□ Usability: ■□□ Transparenz: ■■□	- - -	**C2: Briefwahlverfahren**	- Open-Source-Projekt der Universität Connecticut - Projekt pausiert
Helios	Authentizität: ■□□ Vertraulichkeit: ■□□ Integrität: ■□□ Verh. v. Stimmenkauf: □□□ Verifizierbarkeit: ■■■ Verfügbarkeit: □□□	Aktualität: ■■□ Kosten: ■■□ Usability: ■□□ Transparenz: ■■□	- - -	**C2: Briefwahlverfahren**	- Projekt mit offenem Quellcode - Button „Coerce me!“

Tabelle 5: Gesamtergebnis / Empfehlungskatalog II; C. Paulsen

Ergebnisse / Fazit

- **Kein Verfahren für Ersatz von Präsenzwahlen im politischen (A1) und wirtschaftlichen Umfeld (B1) geeignet**
- **Zwei Verfahren bedingt für Ersatz / Ergänzung der Briefwahl im politischen Umfeld (A2) geeignet (B2: fünf)**
- **Großteil der Verfahren für einen Einsatz in unpolitischen Vereinen (C) bedingt geeignet bzw. geeignet**

Ergebnisse / Fazit

- **Wahlgeräte bieten im Verhältnis zur Papierwahl kaum Vorteile**
- **Ausblick Internetwahlen: Verifizierbarkeit könnte Mehrwert erzeugen**
- **Voraussetzung: Grundsätzlicher Wandel der Internetarchitektur**
- **Nutzung in nichtpolitischen Vereinen als Briefwahlersatz könnte Vorteile bringen**

Ergebnisse / Fazit

- Internetwahlen im politischen Umfeld kurz- und mittelfristig nicht empfehlenswert
- Rechtslage: Fernwahlen als Ausnahme
- Höherer Wirkungsgrad einer Manipulation als bei Papierwahlen
- Wahlen als „Single Point of Failure“ einer Demokratie
- Hauptprobleme: Verfügbarkeitsangriffe, Transparenz / Komplexität, Clientsicherheit
- Demokratischer Akt wird entwertet

Vielen Dank!
Fragen?

Dr. Christian Paulsen
https://www.dfn-cert.de/
paulsen@dfn-cert.de