



# IT-sicherheitstechnische Anforderungen an nicht-politische Online-Wahlen

Berlin, 24.05.2023

Jennifer Koch, BSI

# Gliederung

Einführung in Online-Wahlen

Marktübersicht

Schutzprofil & Technische  
Richtlinie

Fazit & Ausblick



# Einführung in Online-Wahlen



# Einführung in Online-Wahlen

## Online-Wahlen

- Stimmabgabe der Wahlberechtigten mittels elektronischer Eingabegeräte (z.B. Smartphone oder PC) über ein Rechnernetzwerk (z.B. Internet oder Intranet). Weiterleitung und Verarbeitung der Stimmen in einem Online-Wahlsystem.

## Wahlrechtsgrundsätze

- Umsetzung der Wahlrechtsgrundsätze: Allgemein, Direkt, Gleich, Geheim, Frei und Öffentlich in Abhängigkeit von der jeweiligen rechtlichen Grundlage (Wahlverordnung)

## Ende-zu-Ende-Verifizierbarkeit

- Individuelle Verifizierbarkeit
- Universelle Verifizierbarkeit
- Verifizierbarkeit der Berechtigung
- Alle Punkte zusammen werden auch als Ende-zu-Ende Verifizierbarkeit bezeichnet.

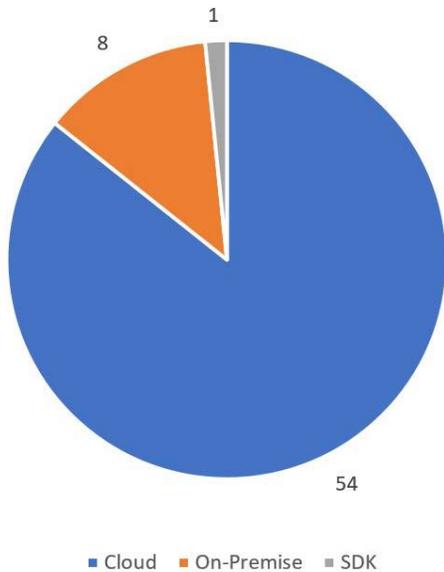


# Marktübersicht

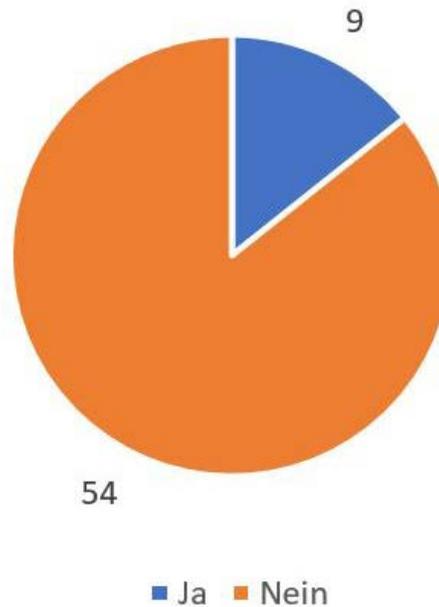
Markt- und Schwachstellenanalyse zur Sicherheit von Online-Wahlprodukten

# Marktübersicht Online-Wahlprodukte

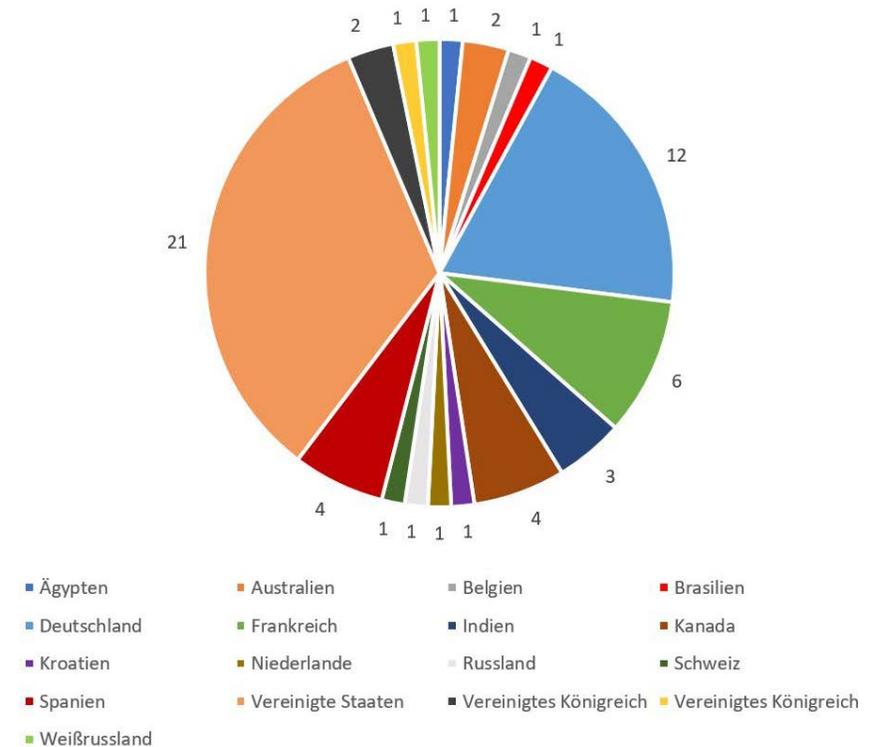
### Produkttyp



### Kryptografische Wahlverfahren



### Firmensitz



# Marktübersicht Online-Wahlprodukte

Auswahl von 5 verschiedenen Online-Wahlprodukten mit unterschiedlichem Produktportfolio für ein repräsentatives Bild der Produktlandschaft

Fokus auf Produkte für die Durchführung von Online-Wahlen (Keine Abstimmungen)

Wahlprodukte mit und ohne kryptografische Wahlverfahren

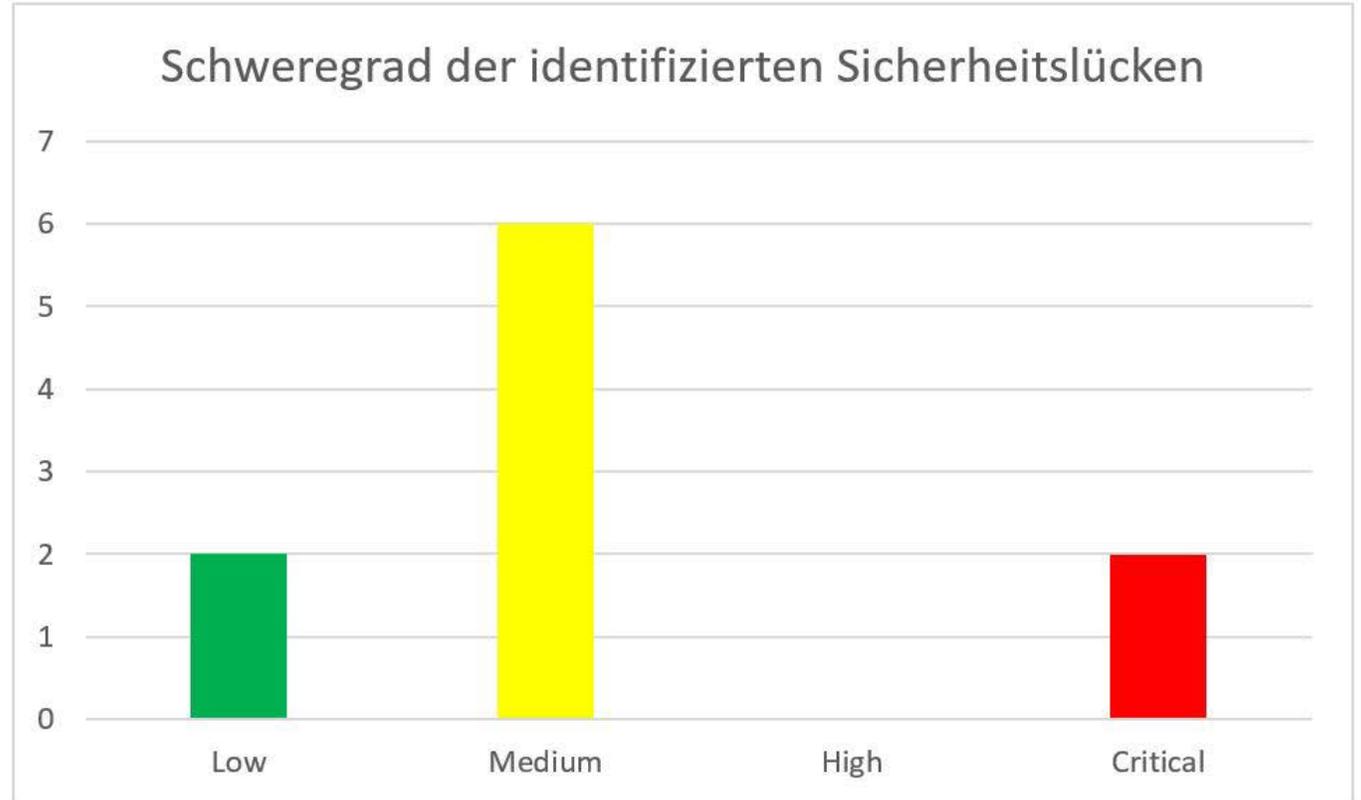
Sowohl proprietäre als auch Open Source Software



„Standard“-Angriffe gegen Webanwendungen, sowie spezifischen Angriffe gegen Online-Wahlen auf Basis von Penetrationstests und Codeanalyse gegen die ausgewählten Produkte

# Marktübersicht Online-Wahlprodukte

- Einstufung nach Common Vulnerability Scoring System (CVSS) in Version 3.1
- Insgesamt 10 gefundene Sicherheitslücken
- Davon „nur“ 2 als Critical einzustufende Sicherheitslücken



# Schutzprofil & Technische Richtlinie

Für nicht-politische Online-Wahlen



# Inhalte des Schutzprofils

IT-sicherheitstechnische Anforderungen an ein Online-Wahlprodukt

Umsetzung kryptografischer Wahlverfahren zur Geheimhaltung der Stimme auch gegenüber dem Betreiber einer Wahl

Umsetzung von Ende-zu-Ende Verifizierbarkeit zur Schaffung von Transparenz in Bezug auf Stimmen und Wahlergebnis

# Herausforderungen

- Umgang mit Fragestellungen, die über das konkrete Produkt hinausgehen
- Notwendigkeit zur Festlegung von Sicherheitsanforderungen zu konkreten Funktionalitäten
- Vergleichbarkeit von Zertifizierungen zu einem Protection Profile, bei der Nutzung von Optionen
- Notwendigkeit zur Gewichtung der Wahlrechtsgrundsätze und daraus resultierende Unterschiede in der Umsetzung



# Ausrichtung der TR-03169



# Zusammenspiel Technische Richtlinie und Schutzprofil

- In welcher Einsatzumgebung wird das Produkt eingesetzt (Verfügbarkeit)?
- Wie identifizieren sich die Wählenden?
- Soll Ende-zu-Ende-Verifizierbarkeit umgesetzt werden?

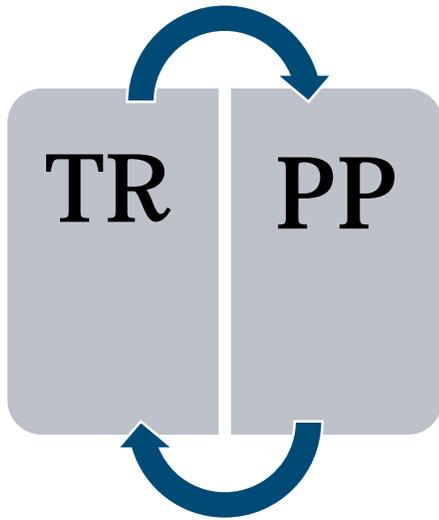


- Ist Re-Voting gewünscht?
- Welchen Schutzbedarf habe ich?
- Welche Risiken gibt es bei einer Online-Wahl?

# Fazit & Ausblick



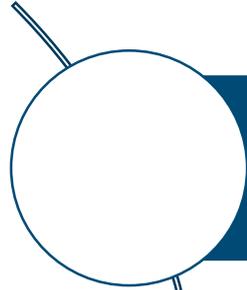
# Fazit



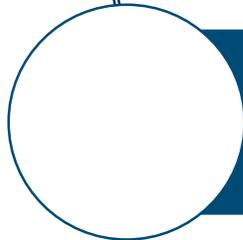
- Standardisierung von Online-Wahlen sind eine Herausforderung
- Dennoch bietet sie eine Chance für Wahlleitungen und auch für Produkthersteller
- Das Zusammenspiel der Dokumente soll eine umfangreiche Unterstützung bieten
- Nichts zu tun ist keine Alternative!



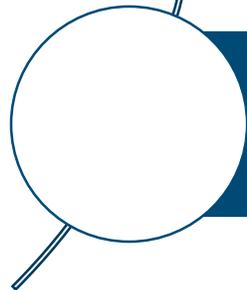
# Ausblick: Projekt StuVe



Studie zu Ende-zu-Ende-Verifizierbarkeitsmethoden für Online-Wahlen



Bisher wird Ende-zu-Ende-Verifizierbarkeit im selben Produkt umgesetzt, wie die Online-Wahl selbst. Daher muss weiterhin dem Betreiber vertraut werden.



Das Projekt soll aus den vielen Umsetzungsmöglichkeiten zur Ende-zu-Ende-Verifizierbarkeit von Online-Wahlen die drei bis fünf geeignetsten in Bezug auf Sicherheit und Marktdurchdringung herausfiltern und die Möglichkeiten einer unabhängigen Verifizierbarkeit aufzeigen.



# Vielen Dank für Ihre Aufmerksamkeit!

## Kontakt

Jennifer Koch (& Sebastian Palm)

[online-wahlen@bsi.bund.de](mailto:online-wahlen@bsi.bund.de)

Bundesamt für Sicherheit in der Informationstechnik (BSI)

Godesberger Allee 185-189

53175 Bonn

[www.bsi.bund.de](http://www.bsi.bund.de)

Deutschland  
**Digital•Sicher•BSI**

Das BSI als die Cyber-Sicherheitsbehörde des Bundes gestaltet Informationssicherheit in der Digitalisierung durch Prävention, Detektion und Reaktion für Staat, Wirtschaft und Gesellschaft.