Bundesamt
für Sicherheit in der
Informationstechnik

Deutschland
Digital•Sicher•BSI•

Anforderungen an Produkte für virtuelle Versammlungen und Abstimmungen

Virtuelle Versammlungen und Abstimmungen (ViVA)

Version 1.0

Änderungshistorie

Version	*Datum*	*Name*	*Beschreibung*
0.5	20.11.2020	Projektteam ViVA	
1.0	19.07.2021	Projektteam ViVA	Ergänzungen, Anpassungen

Bundesamt für Sicherheit in der Informationstechnik
Postfach 20 03 63
53133 Bonn
E-Mail: viva@bsi.bund.de
Internet: https://www.bsi.bund.de/viva

Inhalt

1 Einleitung

Um Versammlungen und Abstimmungen virtuell durchführen und dabei individuelle Anforderungen umsetzen zu können, wird ein Produkt benötigt - zumindest eine Software, ggf. ergänzt durch Hardwarekomponenten. Basierend auf den beiden BSI-Veröffentlichungen "Virtuelle Versammlungen und Abstimmungen" und "Ansätze zur Risikoabwägung bei digitalen geheimen Abstimmungen im Rahmen von Versammlungen"[1] wurde folgender Fragebogen entwickelt. Der Fragebogen listet Eigenschaften für Produkte auf, anhand derer ihre Eignung für virtuelle Versammlungen und Abstimmungen bewertet werden kann. Ergänzend zu den Anforderungen an ein Produkt werden auch Anforderungen an den Dienstleister genannt, wenn die virtuelle Versammlung als Dienst / Service eingekauft wird.

Der Katalog richtet sich somit zuvorderst an Hersteller und Betreiber von Produkten, die für virtuelle Versammlungen und Abstimmungen genutzt werden sollen. Zugleich kann er aber auch eine Orientierungshilfe für Nutzer, Einkäufer/Beschaffer, Betreiber und Administratoren sein, für den jeweils benötigten Anwendungsfall ein geeignetes Angebot auswählen zu können.

Die Beantwortung des Fragebogens durch einen Hersteller stellt keine Produktempfehlung durch das BSI dar. Sie kann zwar ein guter Ansatzpunkt sein, um im Rahmen einer individuellen Risikoanalyse zu evaluieren, ob ein Produkt für einen Einsatzzweck geeignet ist. Eine Garantie für die sichere Umsetzung virtueller Versammlungen und Abstimmungen stellt sie indes nicht dar.

Wir freuen uns,

- wenn uns Hersteller und Betreiber von Produkten zu ihrem Produkt eine Selbstauskunft durch Ausfüllen des Fragebogens zukommen lassen, sodass wir im BSI einen besseren Marktüberblick bekommen und
- wenn Hersteller und Betreiber von Produkten diese Selbstauskunft selbst veröffentlichen oder aber am Produkt Interessierten zur Verfügung stellen, damit diese eine qualifizierte Produktauswahl treffen können.

[1] https://www.bsi.bund.de/DE/Themen/Cyber-Sicherheit/Empfehlungen/Virtuelle_Versammlungen/virtuelle_versammlungen_node.html

2 Produkt und Hersteller / Betreiber

Die folgenden Fragen dienen der Benennung des Produkts, des Produktherstellers und/oder des Dienstbetreibers.

2.1 Produkt

- Name
- Version
- Webadresse (Link zu öffentlich verfügbaren Produktinformationen)

2.2 Hersteller

- Name des Unternehmens
- Unternehmensform
- Sitzland des Unternehmens
- Lokationen der Kundendaten bei Verarbeitung, Sicherung und Speicherung auf Systemkomponenten zur Bereitstellung des Dienstes im Verantwortungsbereich des Anbieters, einschließlich seiner Unterauftragnehmer

2.3 Betreiber (sofern als Dienst angeboten)

- Name des Unternehmens
- Unternehmensform
- Sitzland des Unternehmens
- Lokationen der Kundendaten bei Verarbeitung, Sicherung und Speicherung auf Systemkomponenten zur Bereitstellung des Dienstes im Verantwortungsbereich des Anbieters, einschließlich seiner Unterauftragnehmer

3 Leistungsmerkmale

Im Folgenden soll angegeben werden, welche Leistungsmerkmale das Produkt umfasst (Angabe ja/nein) und, falls relevant, wie diese im Produkt umgesetzt sind (Leistungskennzahlen, Beschreibungen).

3.1 Versammlungen

- Videokonferenz
- Chat-Funktionalität
- Cloud-Lösung zum Dokumentenaustausch bzw. gemeinsamen Arbeiten an Dokumenten
- Teilen des Bildschirms (ScreenSharing)
- Videoübertragung / Streaming (ins Internet) (Wie wird es umgesetzt?)
- Protokollführung / Dokumentation der Veranstaltung (inhaltlich)
- Maximale Teilnehmerzahl

3.2 Abstimmungen

- Funktionalität für Abstimmungen (Wie wird es umgesetzt?)
- Wird verhindert, dass Wahlberechtigungsliste und Stimmberechtigungen während der Wahldurchführung verändert werden können? Wie?
- Können abgegebene Stimmen im Laufe der Wahl korrigiert werden (revoting)? Wie?

3.3 Geheime Abstimmungen

- Funktionalität für geheime Abstimmungen (Wie wird es umgesetzt?)

3.4 Zusätzliche Funktionalität

- Funktionen zur Schaffung von Atmosphäre (Zwischenfragen, Zwischenrufe, Beifall)
- Seitenkommunikationsmöglichkeit für einzelne TeilnehmerInnen (Nebenräume)
- Möglichkeiten zur Erhebung statistischer Daten
- Dolmetscher-Funktion / Gebärdensprache

3.5 Rahmenbedingungen

- Unterstützte Plattformen (Betriebssysteme, Browser, Endgeräte)
- Maßnahmen zur Barrierefreiheit (Schnittstellen, Hilfsmittel)

4 Sicherheitsmerkmale

Im Folgenden soll angegeben werden, welche Maßnahmen das Produkt bzw. der Dienst umgesetzt hat, um die Sicherheitsgrundwerte zu schützen. Hierzu werden beispielhaft Aspekte aufgelistet (Angabe ja/nein) oder Fragen gestellt, zu denen die umgesetzten Maßnahmen erläutert werden sollen. Gerne können Maßnahmen zu weitergehenden Aspekten am Ende ergänzt werden.

4.1 Versammlungen

4.1.1 Verfügbarkeit

- Prävention vor Überlast/Nichterreichbarkeit (z. B. DDoS-Angriffe) von Servern
- Zusätzliche Einwahlmöglichkeit per Telefon (als Rückfallposition)
- Redundante Anbindung der Sitzungsleitung an die zentralen Server
- Notfall-Erreichbarkeit des Betreibers und/oder Herstellers

4.1.2 Authentizität

- Rechte- und Rollenmanagement
  (Welche der Rollen Sitzungsleitung, Protokollierung, stimmberechtigte Teilnahme, nicht stimmberechtigte Teilnahme, Gäste, ZuschauerInnen sind konfigurierbar?)
- Authentisierungsmechanismen (Welche werden unterstützt? Ist eine Multi-Faktor-Authentisierung möglich? Wenn ja, welche?)
- Wie werden Nebenräume vor unbefugtem Betreten abgesichert?

4.1.3 Integrität

- VPN-Nutzung zur Anbindung von TeilnehmerInnen
- Streaming der Versammlung im Internet (zum Erkennen evtl. Manipulationen)

4.1.4 Vertraulichkeit

- Verschlüsselung der Anbindung in der Videokonferenz (Wenn ja, ist es eine Ende-zu-Ende-Verschlüsselung?)
- Wie werden Nebenräume vor unbefugtem Mithören abgesichert?
- Kann die Versammlungsleitung alle anderen TeilnehmerInnen stumm schalten?

4.1.5 Digitale Souveränität

- Ist es möglich, den Server bzw. die gesamte Client-Server-Architektur beim Ausrichter der Versammlung (also "on premise") zu betreiben?

4.1.6 Grundsätzliches

- Wird der "Stand der Technik" für Telemediendienste (z. B. also auch Webseiten, die Online-Abstimmungen anbieten) berücksichtigt?[2]
- Folgt die Grundkonfiguration dem Prinzip "security by default"?
- Werden Anleitungen bezüglich der sicheren Konfiguration angeboten?

[2] https://www.allianz-fuer-cybersicherheit.de/SharedDocs/Downloads/Webs/ACS/DE/BSI-CS/BSI-CS_125.pdf

4.2 Zusätzlich für Abstimmungen

4.2.1 Grundsätzliches

- Ist es möglich, bewusst eine ungültige Stimme abzugeben?
- Welche Vorgaben gibt es an die Nutzer-IT?

4.2.2 Verfügbarkeit

- Wie kann ein Abstimmender der Leitung mitteilen, dass es bei der Abstimmung Probleme gibt (Notfallknopf)?
- Wie geht man vor, wenn ein Teilnehmer nicht abstimmen kann, z. B. weil das Authentisierungsmittel nicht genutzt werden kann (technischer Defekt, Karte verlegt, PIN vertippt)?

4.2.3 Authentizität/Integrität

- Wie werden Mehrfachabstimmungen durch denselben Teilnehmer verhindert?
- Wie wird die Authentizität des Abstimmenden sichergestellt?
- Wie wird sichergestellt, dass die abgegebene Stimme korrekt erfasst und anschließend an die zentralen Systeme übertragen wird?
- Wie wird die Korrektheit der Stimmspeicherung und der Auszählung sichergestellt?
- Wie wird die Korrektheit der Stimmspeicherung und der Auszählung transparent gemacht?
- Müssen sich Abstimmende bei jeder Abstimmung neu authentisieren?
- Wird verhindert, dass ein Zwischenergebnis ermittelt werden kann? Wenn ja, wie?

4.2.4 Transparenz/Nachvollziehbarkeit

- Kann ein Abstimmender im Nachhinein sehen, dass seine Stimme gezählt wurde?
- Kann ein Abstimmender im Nachhinein sehen, ob seine Stimme korrekt gezählt wurde?
- Wie werden Stimmen nach Ende der Abstimmung aufbewahrt?

4.3 Zusätzlich für geheime Abstimmungen

4.3.1 Vertraulichkeit

- Wie wird bei geheimen Abstimmungen sichergestellt, dass niemand erkennen kann, wer wie abgestimmt hat?
    - Wie werden Stimmen und Kennzeichnung des Abstimmenden getrennt?
    - Wie werden die Stimmen verschlüsselt?
- Kann verhindert werden, dass ein Teilnehmer seine Wahlentscheidung beweist? Wenn ja, wie?

4.3.2 Verifizierbarkeit

- Sind Maßnahmen zur Ende-zu-Ende-Verifizierbarkeit umgesetzt? Mit anderen Worten:
    - Ist es möglich, die Korrektheit der Stimmabgabe (cast-as-intended) unabhängig zu überprüfen? Wenn ja, wie?
    - Ist es möglich, die Korrektheit der Stimmaufzeichnung (stored-as-cast) unabhängig zu überprüfen? Wenn ja, wie?
    - Ist es möglich, die Korrektheit der Stimmauszählung (tallied-as-stored) unabhängig zu überprüfen? Wenn ja, wie?

5 Sicherheitsnachweise, Tests und Detektion

Im letzten Block soll noch angegeben werden, wie die Informationssicherheit des Produktes/des Dienstes überprüft und aufrechterhalten wurde/wird.

5.1 Sicherheitsnachweise

- Gibt es eine Auditierung durch unabhängige Stellen? Welche?
- Liegen Zertifizierungen oder eine Zulassung (VS-NfD) des Produkts vor? Welche?
- Liegen Zertifizierungen des Unternehmens (Produkthersteller/Dienstleister) vor? Welche?
- Kommt eine Cloud-Lösung zum Einsatz?
    - Wenn ja: Liegt ein Nachweis zur Einhaltung des BSI C5 in Form eines Testats eines Wirtschaftsprüfers vor?[3]
    - Wenn nein: Liegt eine vertragliche Selbstverpflichtung des Anbieters zur Einhaltung des BSI C5 vor oder, wenn nicht, ist der Anbieter bereit, eine Selbstauskunft zur Einhaltung der C5-Kriterien abzugeben?

5.2 Härtung und Tests

- Wurde das System gehärtet? Wie?
- Sind Penetrationstests oder Revisionen durchgeführt worden? Mit welchem Ergebnis?
- Sind standardisierte Testverfahren angewandt worden? Welche? Mit welchem Ergebnis?

5.3 Monitoring, Fehlerbehandlung, Protokollierung

- Welche Möglichkeiten zur Sicherheitsüberwachung des Systems gibt es vor, während und nach der Abstimmung?
- Gibt es Fehlerbehandlungs- und Protokollierungsmechanismen?

5.4 Umgang mit Schwachstellen/Updates

- Ist der Quellcode des Produkts offen einsehbar?
- Wie geht der Betreiber/Hersteller mit gemeldeten Schwachstellen um (Schwachstellenmanagement)?
- Wie lange werden Sicherheitsupdates für das System angeboten?

[3] www.bsi.bund.de/C5

6 Zusammenfassung

Der obige Fragenkatalog richtet sich an Hersteller und Betreiber von Produkten für virtuelle Versammlungen und Abstimmungen. Zugleich kann er die Produktauswahl erleichtern, in dem er - basierend auf den eigenen Anforderungen - Leistungs- und Sicherheitsmerkmale darstellt.