Anforderungen an Produkte für virtuelle Versammlungen und Abstimmungen

Das Bundesministerium für Sicherheit in der Informationstechnik (BSI) hat einen Fragebogen entwickelt, um Eigenschaften von Produkten zu listen, anhand derer ihre Eignung für virtuelle Versammlungen und Abstimmungen bewertet werden kann. Es dient als Orientierungshilfe und zur Risikoabwägung bei digitalen und geheimen Abstimmungen im Rahmen von Versammlungen für Nutzer und Administratoren.
Die folgende Tabelle listet eine Selbstauskunft des Herstellers der Linkando Software für Formelle Online Meetings. Es wird Produktinteressenten zur Verfügung gestellt, damit diese eine qualifizierte Produktauswahl treffen können.

Linkando erfüllt die Kriterien des BSI in folgendem Maße:

1 Produkt und Hersteller

1.1 Produkt

Name	Linkando
Version	
Webadresse	https://linkando.com/

1.2 Hersteller

Name des Unternehmens	Linkando GmbH
Unternehmensform	GmbH
Sitz	Landau in der Pfalz
Lokationen der Kundendaten	Deutschland

2 Leistungsmerkmale

2.1 Versammlungen

Videokonferenz	Ja
Chatfunktion	Ja
Cloud-Lösung zum Dokumentenaustausch	Ja
Screensharing	Ja
Videoübertragung, Streaming (Wie wird es umgesetzt?)	Es wird das WebRTC Protokoll für die Video-/Audio-übertragung im Web-Browser genutzt.
Protokollführung/ Dokumentation der Veranstaltung (inhaltlich)	Alle technischen und inhaltlichen Informationen die vor und während der Versammlung erstellt werden, werden in ein automatisch generiertes Dokument im .DOCX Format übertragen und stehen nach der Versammlung zum Download bereit.
Teilnehmerzahl	Unlimitiert

2.2 Abstimmungen

Funkionalität für Abstimmungen (Wie wird es umgesetzt?)	Wahlberechtigte Teilnehmer der Versammlung können im Browser online abstimmen. Hierzu wird an die Browser derTeilnehmer zu Beginn einer Wahl oder Abstimmung ein Signal gesendet, dass die Abstimmung eröffnet ist. Nun können die Teilnehmer über Bildschirmtasten abstimmen. Zum Ende der Abstimmung wird wieder ein Signal gesendet, dass die Abstimmung nun geschlossen ist.
Wird verhindert, dass Wahlberechtigungsliste und Stimmberechtigungen während der Wahldurchführung verändert werden können? Wie?	Für jeden Wahlgang ist die Liste der Berechtigten in System hinterlegt. Diese kann vor der Wahl editiert werden, z.B. um eine Befangenheitsausschluss o.ä. vorzunehmen. Alle Änderungen werden nachvollziehbar protokolliert.
Können abgegebene Stimmen im Laufe der Wahl korrigiert werden (revoting)? Wie?	Eine abgegebene Stimme kann solange korrigiert werden, bis sie mit dem Klick des Buttons "Stimme jetzt verbindlich abgeben" final abgegeben wurde.

2.3 Geheime Abstimmungen

Funkionalität für geheime Abstimmungen (Umsetzung)	Bei geheimen Abstimmung wird im System nicht sichtbar, wer wie abgestimmt hat. Hierzu werden die Information der Abstimmungsteilnahme und der Abstimmungseingabe getrennt und verschlüsselt übermittelt, so dass eine Zuordnung der beiden Teile nicht möglich ist.

2.4 Zusätzliche Funktionalität

Funktionen zur Schaffung von Atmosphäre (Zwischenfragen, Zwischenrufe, Beifall)	Zwischenfragen können gestellt werden, in dem man sich über die Schaltfäche "Hand Heben" auf die Sprecherliste setzten lässt. Der Moderator kann die Teilnehmer dann der Reihe nach aufrufen. Zwischenfragen können ebenfalls über den Chat (für alle sichtbar) oder nur ans Backend über "eine Frage stellen" gestellt werden.
Seitenkommunikationsmöglichkeit für einzelne TeilnehmerInnen (Nebenräume)	Ja, es können verschiedene Break-Out Räume mit unterschiedlichen Raumformaten konfiguriert werden.
Möglichkeiten zur Erhebung statistischer Daten	Alle technischen Informationen zu den Verbindungen der Teilnehmer werden protokolliert und können statistische ausgewertet werden, unter Berücksichtigung der Vorgaben der DSGVO.
Dolmetscher-Funktion / Gebärdensprache	Vorhanden

2.5 Rahmenbedingungen

Unterstützte Plattformen (Betriebssysteme, Browser, Endgeräte)	Unsere aktuell unterstützen Plattformen können auf der Seite https://start.linkando.com/videoconferencing jederzeit eingesehen werden. Zudem ist dort auch ein anonymer Selb-Test zum eigenen Browser-System möglich.
Maßnahmen zur Barrierefreiheit (Schnittstellen, Hilfsmittel)	Wir unterstützen Barrierefreiheit über moderne responsive Web technologien, die es behinderten Menschen ermöglichen an unserem Angebot teilzuhaben.

3 Sicherheitsmerkmale

3.1 Versammlungen

3.1.1 Verfügbarkeit

Prävention vor Überlast/Nichterreichbarkeit (z. B. DDoS-Angriffe) von Servern	Ja
Zusätzliche Einwahlmöglichkeit per Telefon (als Rückfallposition)	Optional, bei Anschluss einer zusätzliche Einwahloption.
Redundante Anbindung der Sitzungsleitung an die zentralen Serve	Ja, wenn mehrere Personen die Sitzungsleitung gemeinschaftlich durchführen.
Notfall-Erreichbarkeit des Betreibers und/oder Herstellers	Ja

3.1.2 Authentizität

Rechte- und Rollenmanagement (Welche der Rollen: Sitzungsleitung, Protokollierung, stimmberechtigte Teilnahme, nicht stimmberechtigte Teilnahme, Gäste, ZuschauerInnen sind konfigurierbar?)	Alle
Authentisierungsmechanismen (Welche werden unterstützt? Ist eine Multi-Faktor-Authentisierung möglich? Wenn ja, welche?)	Unterstützung von OAUTH und lokalen verschlüsselten Kennwörtern. MFA optional möglich über die Linkando MFA Lösung (powered by inWebo)
Wie werden Nebenräume vor unbefugtem Betreten abgesichert?	Alle Räumen können nur von zugelassenen Personen "betreten" werden.

3.1.3 Integrität

VPN-Nutzung zur Anbindung von TeilnehmerInnen	Eine VPN Nutzung ist im Zusammenhang mit der WebRTC Videokonferenz nicht möglich. Haben Kunden aber einen VPN-unterstützenden alternative Videokonferenz Dienst, kann dieser per Link als 3rd-Party Videokonferenz genutzt werden.
Streaming der Versammlung im Internet (zum Erkennen evtl. Manipulationen)	Ist möglich

3.1.4 Vertraulichkeit

Verschlüsselung der Anbindung in der Videokonferenz (Wenn ja, ist es eine Ende-zu-EndeVerschlüsselung?)	Ja, es handelt sich um eine Ende-zu-Ende Verschlüsselung
Wie werden Nebenräume vor unbefugtem Mithören abgesichert?	Alle Räumen können nur von zugelassenen Personen "betreten" werden.
Kann die Versammlungsleitung alle anderen TeilnehmerInnen stumm schalten?	Ja, er kann sie sowohl stummschalten, als auch von der Sprecherbühne entfernen.

3.1.5 Digitale Souveränität

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

3.1.6 Grundsätzliches

Wird der "Stand der Technik" für Telemediendienste (z. B. also auch Webseiten, die Online-Abstimmungen anbieten) berücksichtigt?2	Ja
Folgt die Grundkonfiguration dem Prinzip "security by default"?	Ja
Werden Anleitungen bezüglich der sicheren Konfiguration angeboten?	Ja, es gibt sowohl Anleitungsvideos, offene Sprechstunden als auch die möglichkeit des technischen Supports bei der Konfiguration der Versammlung.

3.2 Zusätzlich für Abstimmungen

3.2.1 Grundsätzliches

Ist es möglich, bewusst eine ungültige Stimme abzugeben?	Nein, man kann sich nur enthalten oder gar nicht abstimmen, wenn man keine gültige Stimme abgeben möchte.
Welche Vorgaben gibt es an die Nutzer-IT?	HTTPS Protokoll muss verfügbar sein. zudem dürfen bestimmte DNS Namen für den WebRTC über die Firewall nicht blockiert sein. Die Details sind unserer Dokumentation zu entnehmen.

3.2.2 Verfügbarkeit

Wie kann ein Abstimmender der Leitung mitteilen, dass es bei der Abstimmung Probleme gibt (Notfallknopf)?	Per Chat oder eine "Report a Problem" Taste
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)?	Es gibt die Möglichkeit Stimmen manuell zu ergänzen, wenn diese Option zugelassen wird. Dies kann von der Versammlungsleitung nachvollziehbar durchgeführt werden.

3.2.3 Authentizität/ Integrität

Wie werden Mehrfachabstimmungen durch denselben Teilnehmer verhindert?	Sowohl im Frontend, als auch im Backend kann jeder teilnehmer nur einmal pro Abstimmung abstimmen.
Wie wird die Authentizität des Abstimmenden sichergestellt?	jeder teilnehmer muss sich mit einer Email und einem Kennwort anmelden. Wenn gewünscht können zu Versammlungsbeginn visuelle ID Checks durchgeführt werden.
Wie wird sichergestellt, dass die abgegebene Stimme korrekt erfasst und anschließend an die zentralen Systeme übertragen wird?	Durch eine Ende-zu-Ende Signalstrom zwischen dem Backend der Lösung und den Frontends der Teilnehmer
Wie wird die Korrektheit der Stimmspeicherung und der Auszählung sichergestellt?	Durch Checksummen, Abstimmungsregeln und Protokollierung.
Wie wird die Korrektheit der Stimmspeicherung und der Auszählung transparent gemacht?	Durch Checksummen, Abstimmungsregeln und Protokollierung.
Müssen sich Abstimmende bei jeder Abstimmung neu authentisieren?	Solange eine laufende User Session zwischen dem Backend und dem Frontend der Teilnehmer besteht, ist keine Re-authentifizierung nötig. Bei Abbruch dieser Session muss der Abstimmende sich neu authentifizieren
Wird verhindert, dass ein Zwischenergebnis ermittelt werden kann? Wenn ja, wie?	Bei geheimen oder sogenannten versteckten Abstimmungen kann das Ergebnis er nach Abschluss des Abstimmungsborgangs angezeigt werden. Bei öffentlichen Anstimmungen ist der Zwischenstand jederzeit für alle teilnehmer einsehbar.

3.2.4 Transparenz/ Nachvollziehbarkeit

Kann ein Abstimmender im Nachhinein sehen, dass seine Stimme gezählt wurde?	Er kann sehen, dass die Stimme eingebucht und an das Backend übertragen wurde. Bei offenen Abstimmungen kann er auch nach der Abstimmung sehen, dass seine Stimme gezählt wurde
Kann ein Abstimmender im Nachhinein sehen, ob seine Stimme korrekt gezählt wurde?	Er kann sehen, dass die Stimme eingebucht und an das Backend übertragen wurde. Bei offenen Abstimmungen kann er auch nach der Abstimmung sehen, dass seine Stimme gezählt wurde.
Wie werden Stimmen nach Ende der Abstimmung aufbewahrt?	Bei nicht-geheimen Abstimmungen werden die Stimmen in einer Datenbanktabelle gespeichert. Zudem stehen die Information im Protokoll. Bei geheimen Abstimmungen werden nur die Summen der Abstimmungsergebnisse gespeichert und ins Protokoll geschrieben.

3.3 Zusätzlich für geheime Abstimmungen

3.3.1 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?)	Bei geheimen Abstimmung wird im System nicht sichtbar, wer wie abgestimmt hat. Hierzu werden die Information der Abstimmungsteilnahme und der Abstimmungseingabe getrennt und verschlüsselt übermittelt, so dass eine Zuordnung der beiden Teile nicht möglich ist.
Kann verhindert werden, dass ein Teilnehmer seine Wahlentscheidung beweist? Wenn ja, wie?	Eine 100% verhinderung ist nicht möglich, da ein Teilnehmer seine Abstimmung per Bildschirmfoto "beweisen" könnte, genauso wie es in einer Wahlkabine möglich wäre ein Handyfoto aufzunehmen. Beides verstöst allerdings gegen das Recht oder eine Satzung und könnte bei Bekanntwerden dementsprechend verfolgt werden.

3.3.2 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?	Wir verfügen die Möglichkeit über eine Analyse der Log Dateien und Datenbanken, den Wahlvorgang zu rekonstruieren und entsprechende Nachweise zu erbringen.

4 Sicherheitsnachweise, Tests und Detektion

4.1 Sicherheitsnachweise

Gibt es eine Auditierung durch unabhängige Stellen? Welche?	Es gibt eine PenTest Audizierung der Firma Auxillium Cyber Security. Diese wird in der Regel alle 2 Jahre erneuert. Zudem haben wir unsere Lösungen einen Security Audit durch die Firma Zoom Video Communications durchlaufen lassen.

Liegen Zertifizierungen oder eine Zulassung (VS-NfD) des Produkts vor? Welche?	Nein
Liegen Zertifizierungen des Unternehmens (Produkthersteller/Dienstleister) vor? Welche?	Nein
Kommt eine Cloud-Lösung zum Einsatz? Wenn ja: Liegt ein Nachweis zur Einhaltung des BSI C5 in Form eines Testats eines Wirtschaftsprüfers vor? 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?	Wir nutzen den Cloud Service von Microsoft Azure.

4.2 Härtung und Tests

Wurde das System gehärtet? Wie?	Mithilfe von statischen automatisierten Code Analysen mit dem Tool Snyk und über regelmäßig durchgeführte Penetrationstests.
Sind Penetrationstests oder Revisionen durchgeführt worden? Mit welchem Ergebnis?	Es gibt eine PenTest Audizierung der Firma Auxillium Cyber Security. Diese wird in der Regel alle 2 Jahre erneuert.
Sind standardisierte Testverfahren angewandt worden? Welche? Mit welchem Ergebnis?	Wir wenden das OWASP Verfahren an.

4.3 Monitoring, Fehlerbehandlung, Protokollierung

Welche Möglichkeiten zur Sicherheitsüberwachung des Systems gibt es vor, während und nach der Abstimmung?	Wir haben verschiedene Monitoring Dienst im Einsatz. Aus Sicherheitsgründen nennen wird diese auf Anfrage im Einzelfall.
Gibt es Fehlerbehandlungs- und Protokollierungsmechanismen?	Ja

4.4 Umgang mit Schwachstellen/ Updates

Ist der Quellcode des Produkts offen einsehbar?	Nein
Wie geht der Betreiber/Hersteller mit gemeldeten Schwachstellen um (Schwachstellenmanagement)?	Wir haben einen ITIL orientierten Incident und Change Management Process.
Wie lange werden Sicherheitsupdates für das System angeboten?	Wir nutzen das Verfahren des Continues Delivery. Da es sich um eine reine Cloud Lösung handelt stellen wir keine Sicherheitsupdates bereit.