Bundesamt
für Sicherheit in der
Informationstechnik

Deutschland
Digital•Sicher•BSI•

Virtuelle Versammlungen und Abstimmungen (ViVA)

Ideen und Szenarien für Staat, Wirtschaft und Gesellschaft

Version 1.0

Änderungshistorie

Version	Datum	Name	Beschreibung
0.5	15.06.2020	Projektteam ViVA	Ersterstellung
0.6	06.11.2020	Projektteam ViVA	Ergänzungen, Präzisierungen
1.0	19.07.2021	Projektteam ViVA	Ergänzungen, Präzisierungen, Praxisbeispiel

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

Inhaltsverzeichnis

Änderungshistorie ... 2

1 Einleitung ... 5

2 Erste Schritte ... 6

3 Schutzziele / Schutzbedarf – grundsätzliche Betrachtung der Sicherheitsgrundwerte ... 7

3.1 Verfügbarkeit ... 7

3.2 Authentizität ... 7

3.3 Integrität ... 8

3.4 Vertraulichkeit ... 8

4 Kurze Einführung in IT-Anwendungen für die virtuelle Umsetzung ... 9

4.1 Versammlungen (inkl. Einsicht in Dokumente) ... 9

4.1.1 Videokonferenz-Systeme ... 9

4.1.2 Instant Messaging / Chat-Anwendungen ... 9

4.1.3 Cloud-Lösungen zum Dokumentenaustausch bzw. gemeinsamen Arbeiten an Dokumenten ... 10

4.1.4 Videoübertragung (ins Internet) bei öffentlichen Veranstaltungen ... 10

4.2 Abstimmungen ... 11

4.3 Authentifizierung ... 11

4.4 Technische Basisinfrastruktur ... 12

4.4.1 VPN ... 12

4.4.2 Internetanbindung ... 12

5 Szenarien für virtuelle Sitzungen/Versammlungen ... 13

5.1 Risiken ... 14

5.2 Szenario "klein" – Sitzung mit wenigen TeilnehmerInnen ... 14

5.3 Szenario "mittel" – Sitzung/Versammlung mit bis zu 50 Personen ... 15

5.4 Szenario "groß" – Versammlung mit vielen Personen ... 16

5.5 Schutzmaßnahmen ... 16

5.5.1 Grundsätzlich ... 17

5.5.2 Verfügbarkeit ... 17

5.5.3 Authentizität ... 17

5.5.4 Integrität ... 18

5.5.5 Vertraulichkeit ... 18

6 Szenarien für virtuelle Abstimmungen ... 19

6.1 Risiken ... 19

6.2 Szenario "light" – Abstimmung durch Handheben ... 20

6.3 Szenario "E-Mail" – Abstimmung per E-Mail ... 20

6.4 Szenario "Browser" – Abstimmung in Browser-Anwendung mit transparenter Abstimm-Anzeige ... 20

6.5 Szenario "App" – Umsetzung über Abstimm-App mit transparenter Abstimm-Anzeige ... 20

6.6 Schutzmaßnahmen ... 21

6.6.1 Grundsätzliches ... 21

6.6.2 Verfügbarkeit ... 21

6.6.3 Authentizität ... 22

6.6.4 Integrität ... 22

7 Bausteine zur Ergänzung weiterer Funktionalitäten ... 23

7.1 Atmosphäre (Zwischenfragen, Zwischenrufe, Beifall) 23
7.1.1 zusätzliche Risiken 23
7.1.2 Schutzmaßnahmen 23
7.2 Seitenkommunikation einzelner TeilnehmerInnen 23
7.2.1 zusätzliche Risiken 24
7.2.2 Schutzmaßnahmen 24
7.3 Bereitstellung von Dokumenten / Kollaborationen 24
7.3.1 zusätzliche Risiken 25
7.3.2 Schutzmaßnahmen 26
7.4 Protokollierung / Dokumentation 26
7.4.1 zusätzliche Risiken 26
7.4.2 Schutzmaßnahmen 26
7.5 Dolmetschen / Gebärdensprache 26
7.5.1 zusätzliche Risiken 27
7.5.2 Schutzmaßnahmen 27
7.6 Übertragung der Versammlung ins Internet (Öffentlichkeit) 27
7.6.1 zusätzliche Risiken 27
7.6.2 Schutzmaßnahmen 28
7.7 Geheime Abstimmung 28
8 Bausteine für höheren Schutzbedarf 29
8.1 Schutzbedarf hoch bzgl. Verfügbarkeit 29
8.1.1 zusätzlich adressierte Risiken 29
8.1.2 Schutzmaßnahmen 29
8.2 Schutzbedarf hoch bzgl. Authentizität 29
8.2.1 zusätzlich adressierte Risiken 29
8.2.2 Schutzmaßnahmen 29
8.3 Schutzbedarf hoch bzgl. Integrität 30
8.3.1 zusätzlich adressierte Risiken 30
8.3.2 Schutzmaßnahmen 30
8.4 Schutzbedarf hoch bzgl. Vertraulichkeit 30
9 Praxisbeispiel Parteitage 31
9.1 zusätzliche Risiken 32
9.2 Schutzmaßnahmen 32
10 Zusammenfassung und Aufruf zur Kommentierung 34

1 Einleitung

Die derzeitige Pandemiesituation bringt viele Organisationen dazu, Alternativen zu bisher üblichen Versammlungsformen zu suchen - sei es wegen rechtlicher Vorgaben, aus Präventionsgründen, durch selbst gewählte Einschränkungen bzgl. größerer Menschenansammlungen oder aber aus Gründen der Nachhaltigkeit. Allgemein wird erwartet, dass die neuen Formen von virtuellen Versammlungen auch nach Ende der Pandemie im sogenannten New Normal fortbestehen werden. Die IT-Entwicklung und -Vernetzung hat einen Stand erreicht, Online-Formen von Versammlungen grundsätzlich technisch zu ermöglichen - angefangen von der Besprechung/Sitzung mit wenigen TeilnehmerInnen bis hin zu Versammlungen mit mehr als 1.000 TeilnehmerInnen und zugeschalteter Öffentlichkeit. Auch rechtlich wurden Regelungen erlassen, um die Online-Durchführung zu ermöglichen oder zu erleichtern, z. B. bei Mitglieder- oder Aktionärsversammlungen. Doch wie lassen sich diese Szenarien realisieren? Worauf ist zu achten, damit Informationen sicher übertragen und ausgetauscht werden können? Im vorliegenden Papier geben wir auf diese Fragen anhand von Ideen und Szenarien erste Antworten, um damit die Umsetzung in Staat, Wirtschaft und Zivilgesellschaft zu unterstützen.

Der vorliegende Text ist wie folgt gegliedert: Zu Beginn werden grundlegende Ausführungen zur Vorgehensweise, zu Schutzzielen der Informationssicherheit und zum Thema Schutzbedarf gemacht. Auch erfolgt eine kurze Erläuterung zu den im Kontext virtueller Versammlungen und Abstimmungen benötigten IT-Systemen und -Anwendungen. Anschließend werden in zwei Abschnitten Umsetzungsmöglichkeiten beschrieben, zum einen für virtuelle Versammlungen, zum anderen für virtuelle Abstimmungen. Daran schließen sich Beschreibungen einzelner Funktionalitäten in Form von Bausteinen an, beschrieben mit ggf. zusätzlich betrachteten Risiken und Maßnahmen. Nach Empfehlungen für einen höheren Schutzbedarf wird abschließend noch das Praxisbeispiel Parteitage dargestellt.

Die Veröffentlichung erhebt keinen Anspruch auf Vollständigkeit. Sie möchte aber eine Hilfestellung für die unterschiedlichen Zielgruppen in

- Zivilgesellschaft (z. B. Mitgliederversammlungen von Vereinen, Arbeitsgruppen)
- Wirtschaft (z. B. Aktionärsversammlungen/Hauptversammlungen)
- Politik (z. B. Parteitage, kommunale politische Gremien)
- Öffentliche Verwaltung (z. B. Sitzungen, Beratungen und Workshops innerhalb und zwischen Gebietskörperschaften)

u.a.m. anbieten.

2 Erste Schritte

Wenn Sie sich aufmachen, Ihre bisher physisch durchgeführten Treffen in die Online-Welt zu verlegen, sollten Sie als Erstes Ihre Anforderungen zusammenstellen, sowohl aus funktionaler wie organisatorischer Sicht als auch im Hinblick auf die Informationssicherheit und deren Schutzziele Vertraulichkeit, Verfügbarkeit, Integrität, aber insbesondere auch Authentizität. Typische Fragen können sein:

- Wie läuft die jetzt online abzubildende Versammlung bisher ab? Wer nimmt teil? Wer hat welche Rolle?
- Welche (notwendigen/üblichen/sinnvollen) Kommunikationselemente gibt es neben der offiziellen Versammlung (z. B. Pausengespräche, informelle Absprachen in Zwiegesprächen während der Versammlung)?
- Welche Beschränkungen gibt es derzeit (z. B. Teilnahme beschränkt auf definierten Personenkreis, Versammlung öffentlich/nicht-öffentlich, wer hat Rederecht usw.)?
- Welche der o. g. Abläufe und Rahmenbedingungen müssen auch in der virtuellen Variante erhalten bleiben? Welche können verändert werden? Auf welche kann verzichtet werden?
- Welcher Schutzbedarf besteht bzgl. Verfügbarkeit, Vertraulichkeit, Integrität sowie Authentizität?

Ziel einer Online-Umsetzung von Versammlungen und Abstimmungen muss es sein, das Online-"Erlebnis" möglichst so zu gestalten, dass es alle wichtigen Aspekte der persönlichen Zusammenkünfte abbildet. Einen Gedanken möchten wir jedoch von Beginn an mitgeben:

Hinterfragen Sie die bisherigen Abläufe kritisch und suchen Sie nach Verbesserungspotential. Nur weil gewisse Abläufe in den bisher physisch gelebten Prozessen immer so waren, heißt es nicht, dass sie unumstößlich sind. Versucht man alles Physische eins zu eins online abzubilden, so wird die Umsetzung häufig sehr kompliziert. Vereinfachen Sie zunächst die Prozesse so gut wie es geht (ohne Wesentliches zu verlieren) und überlegen Sie sich dann die digitale Umsetzung. Dies gilt insbesondere auch für Fragen der Absicherung Ihrer Prozesse: Typisches Beispiel aus dem E-Government ist die händische Unterschrift, die in der Papier-Welt völlig üblich ist, aber nur sehr selten wirklich benötigt wird, und daher auch nur sehr selten in der Online-Welt durch ein rechtssicheres Äquivalent umgesetzt werden muss. Denken Sie so pragmatisch wie möglich und zugleich so sicher wie nötig.

3 Schutzziele / Schutzbedarf – grundsätzliche Betrachtung der Sicherheitsgrundwerte

Klassischerweise werden die Schutzziele Vertraulichkeit, Integrität und Verfügbarkeit betrachtet. Es gibt darüber hinaus weitere Ziele, die im Kontext virtueller Versammlungen und Online-Abstimmungen Relevanz besitzen. Für die genannten Schutzziele muss das zu erreichende Sicherheitsniveau, also der Schutzbedarf, festgelegt und in der Konzeption mit Maßnahmen adressiert werden. Die Einhaltung eines bestimmten Sicherheitsniveaus erfordert stets finanzielle, personelle und zeitliche Ressourcen, die von der Leitungsebene ausreichend bereitgestellt werden müssen.

Zur Erstellung des Sicherheitskonzepts empfiehlt das BSI grundsätzlich die Anwendung des IT-Grundschutzes des BSI[1]. Je nach Größe und Bedeutung der umzusetzenden Versammlung kann hierbei sehr pragmatisch vorgegangen werden, perspektivisch könnte auch ein IT-Grundschutz-Profil[2] "Virtuelle Versammlungen und Abstimmungen" erstellt werden. Das BSI unterstützt einen Prozess zur Erstellung eines solchen Profils gerne.

Falls bzgl. einzelner Sicherheitsgrundwerte der Schutzbedarf hoch ist, ist zur Ergänzung der Standard-Schutzmaßnahmen eine ergänzende Risikoanalyse erforderlich. Einige bei hohem Schutzbedarf offensichtliche Risiken werden am Ende dieses Dokuments bereits aufgelistet, sie ersetzen aber nicht eine systematische Herangehensweise im Verlauf der eigenen Planung und Umsetzung. Auch sollte eine neu konzipierte und aufgebaute IT stets einer Überprüfung vor Erstnutzung unterzogen werden, z. B. durch Penetrationstests, Revisionen oder Webchecks. Nur so kann festgestellt werden, ob das im Sicherheitskonzept vorgegebene Sicherheitsniveau auch tatsächlich erreicht und gehalten wurde.

3.1 Verfügbarkeit

Offensichtlich ist für die Durchführung einer Online-Versammlung die Verfügbarkeit sicherzustellen. So gilt es, System- und Kommunikationsausfälle zu verhindern. Zu beachten ist hier, dass die Verfügbarkeit an drei unterschiedlichen Stellen gewährleistet sein muss:

- an den zentralen Komponenten/Systemen (des Veranstalters oder der einladenden Organisation),
- bei der Kommunikationsverbindung (Internet, Festnetz- oder Mobiltelefonie) sowie
- bei den dezentralen Endgeräten (Mobiltelefone, PCs, Laptops).

Im Kontext der Verfügbarkeit sollten ggf. auch die **Resilienz und Widerstandsfähigkeit,** also der Umgang mit bzw. die Belastbarkeit gegenüber Störungen, mit betrachtet werden. Beispielsweise muss die Teilnahme an Abstimmungen auch noch möglich und verifizierbar sein, wenn die Videoübertragung der Versammlung gestört ist. Eine Entkopplung der Kanäle für Versammlung und Abstimmung wäre hier eine Möglichkeit.

3.2 Authentizität

Die Teilnahme an Versammlungen, und insbesondere an Abstimmungen in diesen Versammlungen, ist häufig nur einer konkreten Personengruppe erlaubt (wie z. B. Mitglieder, Stimmberechtigte). Bei der Online-Abbildung von Versammlungen muss daher ein Mechanismus bestehen, der die TeilnehmerInnen authentisiert, sprich sicherstellt, dass eine berechtigte Person in einer Online-Versammlung auch wirklich persönlich anwesend ist und ihre Stimme(n) bei Abstimmungen persönlich abgibt. Dabei hängt der Schutzbedarf bzgl. der Authentisierung stark von der Art der Versammlung ab, er ist im Konzept festzulegen.

1 https://www.bsi.bund.de/IT-Grundschutz
2 https://www.bsi.bund.de/DE/Themen/Unternehmen-und-Organisationen/Standards-und-Zertifizierung/IT-Grundschutz/IT-Grundschutz-Profile/it-grundschutz-profile_node.html

Im Kontext der Authentizität sollten ggf. auch die Sicherheitsgrundwerte **Verbindlichkeit und Zurechenbarkeit/Nicht-Abstreitbarkeit** mit betrachtet werden, also der Aspekt, Handlungen einem Teilnehmenden sicher zuzuordnen.

3.3 Integrität

Oft übersehen, ist die Integrität eines der wichtigsten Schutzziele im Kontext von Versammlungen und Abstimmungen. Es geht darum, dass die Redebeiträge und Abstimmungsvoten (also die Informationen) unverfälscht übertragen werden. In Zeiten von fake news und der Möglichkeit, auch Bilder und Videos so zu manipulieren, dass es nicht ohne tiefere technische Analyse auffällt (Deep Fakes, Morphing), sollte im Konzept ein besonderer Fokus auf diesem Schutzziel liegen.

3.4 Vertraulichkeit

In vielen Versammlungen sind die Inhalte der Kommunikation nicht vertraulich, d. h. entweder sind die Versammlungen ohnehin öffentlich oder aber es ist kein Problem, wenn Informationen an die Öffentlichkeit gelangen. Sofern jedoch Dinge intern, also ausdrücklich nicht-öffentlich, behandelt werden sollen, muss das Schutzziel Vertraulichkeit in der Konzeption von Anbeginn an mit berücksichtigt werden.

Ein Hinweis zur Abgrenzung: In dem vorgelegten Papier betrachten wir ausschließlich den Umgang mit offenen oder organisationsinternen Unterlagen und Themen. Ausdrücklich nicht betrachtet werden Besprechungen zu nach VS-Anweisung[3] eingestuften Informationen.

Besonders relevant ist Vertraulichkeit zudem bei geheimen Abstimmungen. Hier ist es zwingend erforderlich, dass die notwendige Authentisierung des Abstimmenden (zur Überprüfung der Stimmberechtigung) von der authentisierten Information (dem Abstimmungsvotum) entkoppelt werden kann. Das Thema geheime Abstimmungen ist jedoch nicht Teil dieser Veröffentlichung – es wird in der BSI-Veröffentlichung "Ansätze zur Risikoabwägung bei digitalen geheimen Abstimmungen im Rahmen von Versammlungen"[4] adressiert..

Im Kontext der Vertraulichkeit sollte ggf. auch die **Kontingenz** mit betrachtet werden, also dass eine technische Umsetzung nicht mehr Informationen erhebt und offenbart als die analoge Variante. Hierzu muss berücksichtigt werden, welche Metainformationen bei einer technischen Realisierung anfallen, und überprüft werden, ob diese mit den spezifischen Regeln der Versammlung vereinbar sind. Es ist zu prüfen, ob und wann Änderungen hinsichtlich der wahrnehmbaren Informationen in Ordnung sind und wann nicht. Kontingenz ist in erster Linie ein Aspekt des Datenschutzes.

3 https://www.bsi.bund.de/DE/Themen/Oeffentliche-Verwaltung/Geheimschutz/Geheimschutzberatung/VorschriftenStandards/vorschriftenstandards_node.html
4 https://www.bsi.bund.de/viva

4 Kurze Einführung in IT-Anwendungen für die virtuelle Umsetzung

Um virtuelle Versammlungen und Abstimmungen durchführen zu können, wird es in der Regel möglich sein, auf Standard-IT zurückzugreifen. Im Folgenden werden die wesentlichen Elemente kurz vorgestellt.

4.1 Versammlungen (inkl. Einsicht in Dokumente)

4.1.1 Videokonferenz-Systeme

Moderne Videokonferenzlösungen bieten die Möglichkeit, Veranstaltungen mit bis zu vielen Tausend ZuschauerInnen durchzuführen. Die entsprechenden Funktionalitäten werden mit den Schlagworten "Events" oder "Webinar" beworben. Zu beachten ist, dass ein Unterschied gemacht wird zwischen ZuschauerInnen und TeilnehmerInnen. Während die Rolle der ZuschauerInnen passiv ist, sie können die Vorträge nur verfolgen, d. h. ihnen wird nur der Video- und Audiodatenstrom übermittelt, ist die Rolle der TeilnehmerInnen aktiv. Sie können z. B. durch einen eigenen Wortbeitrag in den Ablauf eingreifen. Die Zahl der TeilnehmerInnen liegt abhängig vom Produkt bei wenigen Hundert. Dem vortragenden Teilnehmer stehen Funktionen ("Präsentation" oder "Desktop Sharing") zur Verfügung, um Dokumente zu präsentieren.

Besteht Bedarf den Zugang zur virtuellen Versammlung auf bestimmte TeilnehmerInnen zu beschränken, muss den Mechanismen der Videokonferenzlösung zur Zutrittskontrolle besondere Beachtung geschenkt werden. Hier haben sich verschiedene Verfahren etabliert, die in manchen Lösungen auch kombiniert werden. Ein Ansatz ist der "Einladungs-Link" ("invitation link"), der die Nummer des virtuellen Konferenzraumes enthält. Die Länge der Nummer sollte so gewählt werden, dass sie nur schwer zu erraten ist. Der Link wird dann auf einem sicheren Kanal an die gewünschten TeilnehmerInnen verteilt. Der Link kann auch veröffentlicht werden, wenn sich der Raum durch eine PIN absichern lässt. Dann muss lediglich die PIN auf einem sicheren Kanal übermittelt werden. Ein anderer Ansatz ist die Verwendung einer Wartezone, aus der den TeilnehmerInnen nach Identifikation durch die Moderation Zutritt in den Konferenzraum gewährt wird. Letzte Maßnahmen der Zutrittskontrolle sind der Ausschluss eines Teilnehmers oder die "Verriegelung" des Konferenzraums durch die Moderation.

4.1.2 Instant Messaging / Chat-Anwendungen

Chat-Anwendungen bzw. Instant Messenger können als schnelles Echtzeit-Kommunikationsmedium genutzt werden. Hierbei tauschen zwei oder mehr TeilnehmerInnen mithilfe der jeweiligen Software Textnachrichten aus. Häufig erfolgen hierzu zunächst Registrierungen nach Installation der Software. Die Ausgestaltung der Authentisierung ist dabei variabel. Chatfunktionen finden sich häufig auch in Diensten, die beispielsweise vornehmlich als Videokonferenzdienst gestaltet sind. Dies ermöglicht eine breite Interaktion zwischen den einzelnen TeilnehmerInnen. Hier zeigen sich auch die Vorteile für virtuelle Versammlungen: Da außer einem mit dem Internet verbundenen Endgerät und der jeweiligen Anwendung keine weitere Hardware, wie Kamera oder Mikrofon, zwingend benötigt wird, bieten Chat-Anwendungen bzw. integrierte Chatfunktionen die Chance, einer großen Anzahl an Personen niedrigschwelligen und unkomplizierten Zugang zu virtuellen Versammlungen zu ermöglichen.

4.1.3 Cloud-Lösungen zum Dokumentenaustausch bzw. gemeinsamen Arbeiten an Dokumenten

Es gibt eine Vielfalt an Lösungen, darunter auch Open-Source-Software, welche einerseits das Teilen (Sharing) und andererseits das kollaborative Bearbeiten von Dokumenten in Echtzeit ermöglicht.

- Sharing-Plattformen bieten den Vorteil, dass jegliche Arten von Dateiformaten unterstützt werden, d. h. Fotos, PDFs, Office-Dokumente etc. können gleichermaßen einer Gruppe von Personen zugänglich gemacht werden. Diese Dokumente können dann mit den gewohnten Programmen bearbeitet werden. Änderungen werden entweder beim Abspeichern, in regelmäßigen Abständen oder auf manuelle Intervention hin allen anderen TeilnehmerInnen verfügbar gemacht. Ein Versionshistorie macht zudem sichtbar, wer das Dokument zuletzt zur Verfügung gestellt hat, und z. T. auch, wer die Datei heruntergeladen hat. Die Kompatibilität mit allen Formaten bringt aber den Nachteil mit sich, dass gleichzeitiges Bearbeiten desselben Dokuments grundsätzlich nicht möglich ist. Es stehen bekannte kommerzielle Lösungen zur Verfügung, aber auch Open-Source-Software spielt bei Sharing Diensten eine große Rolle.
- Lösungen für Echtzeit-Kollaboration sind maßgeschneiderte Software, die das gemeinsame und gleichzeitige Bearbeiten bestimmter Dokumentenformate ermöglicht. Der einfachste Fall ist hierbei eine Website, die allen Kooperationspartnern ein Fenster mit Text darstellt, welcher von allen gleichzeitig bearbeitet und (rudimentär) formatiert werden kann. Es gibt bewährte und weit verbreitete Produkte, die eine Verschlüsselung bieten und sicherstellen, dass der Dienstbetreiber keine Einsicht in die verarbeiteten Daten nehmen kann. Darüber hinaus existieren Produkte, die die gleichzeitige Bearbeitung von Office-Dokumenten (Texte, Tabellenkalkulation, Präsentationen) ermöglichen. Es stehen kommerzielle wie auch Open-Source-Lösungen zur kollaborativen Echtzeit-Bearbeitung von Office-Dokumenten zur Verfügung – auch der gängigen proprietären Dateiformate. Der Funktionsumfang reicht in der Regel nicht an den der Desktop-Office-Suiten heran, bietet aber weit mehr Gestaltungsmöglichkeiten als die eingangs aufgeführten Lösungen. Zum Speichern und Verteilen der Dokumente ist dann in der Regel noch eine Sharing-Plattform, wie oben beschrieben, notwendig.

4.1.4 Videoübertragung (ins Internet) bei öffentlichen Veranstaltungen

Bei der Übertragung von virtuellen Versammlungen an ein breites Publikum ist zwischen der Produktion der Aufnahmen und der Übertragung an die ZuschauerInnen zu unterscheiden. Bei der Produktion vor Ort gibt es eine große Bandbreite verschiedener Möglichkeiten. So kann auf der einen Seite mit relativ wenig Aufwand der Datenstrom einer Videokonferenz, einer Videokamera bzw. eines Mobiltelefons verwendet werden, um eine Quelle für eine Live-Aufnahme zu bekommen. Auf der anderen Seite des Spektrums stehen aufwendig produzierte Live-Aufnahmen, die als Dienstleistung von Produktionsfirmen eingekauft werden können, mit verschiedenen Kameras, Schnitten und Einspielern.

Für die Übertragung an die ZuschauerInnen kann auf existierende Plattformen zurückgegriffen werden, die z. B. originär für das Live-Streaming von Computerspielen oder Konferenzen entwickelt und verwendet wurden. Ansonsten können Aufwand und Kosten mit wachsender Teilnehmerzahl für den Veranstalter einer Versammlung als Sender des Videosignals steigen, da die Daten an jeden Empfänger einzeln versandt werden müssen. Hier überschreiten handelsübliche Internetanschlüsse eines Veranstalters schnell ihre Kapazitätsgrenzen.

Wird eine Veranstaltung über einer Streaming-Plattform live auf die Website eines Veranstalters übertragen (Livestreaming), muss der Veranstalter bei dem von ihm genutzten Streaming-Kanal entsprechende Sicherheitseinstellungen berücksichtigen (z. B. sicheres Passwort, Zwei-Faktor-Authentifizierung für das Bereitstellen des Streams auf der Plattform). Die Redundanz bei der öffentlichen Übertragung einer Veranstaltung ins Internet lässt sich erzielen, wenn die Veranstaltung gleichzeitig auf unterschiedlichen, voneinander unabhängigen Streaming-Kanälen übertragen wird (Multiplattform-Streaming).

4.2 Abstimmungen

Online-Abstimmungen werden auf privater Ebene bereits genutzt und sind auch Bestandteil von sozialen Medien. Die Anwendungsgebiete sind dabei vielfältig und reichen von Terminfindung für gemeinsame Unternehmungen in einer Gruppe bis hin zu kurzen, nicht repräsentativen Meinungsbildern. In virtuellen

Versammlungen können entsprechende Tools in die verwendete Plattform integriert werden, um zuvor diskutierte Themen zu einer demokratischen Entscheidung zu bringen. Dies unterstützt Gruppen und Vereinigungen dabei, auch im virtuellen Raum nachvollziehbare Beschlüsse treffen zu können.

Darüber hinaus gibt es auch verschiedene Anbieter professioneller Lösungen für Online-Abstimmungen, die verschiedene Sicherheitsanforderungen erfüllen, bis hin zu geheimen Abstimmungen.

4.3 Authentifizierung

Um eine sichere und vertrauenswürdige Kommunikation zwischen den TeilnehmerInnen einer Online-Versammlung zu ermöglichen, müssen Mechanismen zur sicheren Identifizierung der TeilnehmerInnen bereitstehen. Die Identität einer natürlichen oder juristischen Person wird durch verschiedene Eigenschaften beschrieben, wie beispielsweise Name, Anschrift, Geburtsdatum, E-Mail-Adresse oder auch Pseudonym. In der virtuellen Welt werden Namen und Eigenschaften durch Attribute einer elektronischen Identität abgebildet.

Um den Zugang zu einer Online-Versammlungs-Plattform zu ermöglichen, muss ein Nutzer erkennbar sein, d. h. bestimmte Identitätsinformationen müssen dem System zur Verfügung gestellt werden. Für die sichere Nutzung ist die Authentizität dieser Identitätsdaten von entscheidender Bedeutung. Sind diese gefälscht, veraltet oder nicht nachweisbar, kann auch eine sichere Infrastruktur keine vertrauenswürdige Kommunikation erzeugen.

Bei der Registrierung mit einer E-Mail-Adresse bei einem Online-Videokonferenz-Tool gilt es zu beachten, dass die Nutzung einiger dieser Plattformen direkt mit einem persönlichen Nutzerkonto bei bestimmten Technologieunternehmen (z. B. im Kontext der Betriebssysteme von Microsoft, Apple oder Google) verknüpft ist, das wiederum die Nutzung weiterer Services ermöglicht. Um zu verhindern, dass unberechtigte Personen Zugriff auf solche Accounts und den damit verbundenen Funktionen und Nutzungsmöglichkeiten erhalten, sind auch hier die Empfehlungen für eine sichere Authentifizierung zu beachten (z. B. sichere Passwörter, Zwei-Faktor-Authentifizierung, keine Weitergabe von Passwörtern an andere Personen). Damit wird das Maß an Sicherheit insgesamt deutlich erhöht.

Hat sich ein Nutzer authentisiert, so muss das System vorgeben, was dieser Nutzer darf. Die Autorisierung umfasst die Zuweisung und Überprüfung von Zugriffsrechten auf Daten, Dienste und Ressourcen. Auf Basis der Authentisierung und festgestellten Autorisierung können nun Prozesse, wie die Teilnahme an einer Besprechung oder Abstimmung, initiiert und durchgeführt werden.

Die Plattform sollte für die elektronische Identifizierung des Nutzers ein Verfahren einsetzen, mit dessen Hilfe sie die Identität auf einem für die Versammlung oder Abstimmung geeigneten Vertrauensniveau feststellen kann. Die Technische Richtlinie BSI TR-03107[5] definiert hierfür im ersten Teil Kapitel 2.3 "Vertrauensniveaus" drei Niveaus, um verschiedene Schutzbedürfnisse abzudecken.

Zur Auswahl geeigneter Identifizierungsverfahren können die Vorgaben für das entsprechende Vertrauensniveau gemäß der BSI TR-03107 zu Rate gezogen werden. Das Verfahren zur elektronischen Identifizierung sollte hierbei insbesondere die Anforderungen gemäß BSI TR-03107 Kapitel 5 „Identifizierung“ für die Identifizierung der Person und gemäß BSI TR-03107 Kapitel 4 „Authentisierungsverfahren“ für Authentisierung während der Anmeldung des Nutzers an der Plattform erfüllen.

Zum Erreichen des Vertrauensniveaus normal reichen die Verwendung eines geeigneten Nutzernamens und eines sicheren Passworts.

5 https://www.bsi.bund.de/DE/Themen/Unternehmen-und-Organisationen/Standards-und-Zertifizierung/Technische-Richtlinien/TR-nach-Thema-sortiert/tr03107/TR-03107_node.html

4.4 Technische Basisinfrastruktur

4.4.1 VPN

Virtuelle Private Netze (VPN - Virtual Private Network) bieten die Möglichkeit einer verschlüsselten Kommunikation zwischen verschiedenen Rechnern oder Standorten. Hierzu wird ein verschlüsselter Tunnel aufgebaut, typischerweise zwischen einem Endgerät/Client und einem Server. Der Aufbau eines Tunnels kann über verschiedene Techniken erfolgen. Die gebräuchlichsten VPN-Techniken und deren Sicherheitseigenschaften werden in der BSI-Studie „Aufbau von Virtual Private Networks (VPN) und Integration in Sicherheitsgateways“[6] beschrieben. Weitere Informationen rund um den Fernzugriff, wie Authentisierung, finden sich in der BSI-Studie „ISi-Fern“[7].

4.4.2 Internetanbindung

Die Internetanbindung des Konferenzsystems muss ausreichend dimensioniert sein. Bei hohen Verfügbarkeitsanforderungen ist eine redundante Anbindung über unabhängige Anbieter und Leitungen zu erwägen (siehe im BSI-IT-Grundschutz-Baustein NET.1.1[8]). Grundlegende Informationen zur Anbindung von Netzen in das Internet finden sich in der BSI-Studie „ISi-LANA“[9].

Bei der Kapazitätsplanung der Internetanbindung muss auch die Möglichkeit von Distributed-Denial-of-Service-Angriffen (DDoS-Angriffen) betrachtet werden. Mit solchen DDoS-Angriffen lassen sich vorhandene Leitungskapazitäten oft ausschöpfen, sodass es zu Engpässen kommen kann. Zur Vorbereitung auf DDoS-Angriffe sollte mit den gewählten Internetanbietern und ggf. mit dedizierten DDoS-Mitigation-Dienstleistern gesprochen werden. Unabhängig von der Internetanbindung gibt es auch DDoS-Angriffe, die nicht auf die Leitung, sondern auf einen angebotenen Dienst (etwa ein Konferenzsystem) abzielen. Zahlreiche Informationen zur Prävention und Mitigation von DDoS-Angriffen finden sich auf der BSI-Themenwebseite zu DDoS[10].

6 https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Internetsicherheit/vpn_pdf.html
7 https://www.bsi.bund.de/DE/Themen/Unternehmen-und-Organisationen/Informationen-und-Empfehlungen/ISI-Reihe/isi-reihe_node.html#doc453736bodyText3
8 https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Grundschutz/Kompendium_Einzel_PDFs_2021/09_NET_Netze_und_Kommunikation/NET_1_1_Netzarchitektur_und_design_Edition_2021.pdf
9 https://www.bsi.bund.de/DE/Themen/Unternehmen-und-Organisationen/Informationen-und-Empfehlungen/ISI-Reihe/isi-reihe_node.html#doc453736bodyText2
10 https://www.bsi.bund.de/ddos

5 Szenarien für virtuelle Sitzungen/Versammlungen

Besprechungen und Versammlungen (im Folgenden beides unter dem Begriff Versammlungen zusammengefasst) finden in den unterschiedlichsten gesellschaftlichen Gruppen, in diversen Größen und mit verschiedensten Zielsetzungen statt. Im Folgenden wird versucht, diese Vielfalt in einige wenige Grundszenarien zusammenzufassen, sodass jede Leserin und jeder Leser sich das am besten passende Szenario als Ausgangspunkt auswählen kann. Dabei bauen die drei Szenarien aufeinander auf. Aspekte, die z. B. schon im ersten Szenario beschrieben sind, werden in den folgenden Szenarien als gegeben vorausgesetzt, sofern hier nicht ausdrücklich etwas anderes beschrieben bzw. empfohlen wird.

Im Anschluss werden dann ergänzende Aspekte in Form von Bausteinen beschrieben, die zum Grundszenario hinzugefügt werden können.

- Allen Szenarien ist gleich, dass sich eine Gruppe von Menschen virtuell treffen möchte, um entlang einer Tagesordnung, ggf. auf der Basis von vorgelegten Unterlagen, Themen zu diskutieren und zu einzelnen Punkten Beschlüsse zu fassen, die durch Abstimmungen herbeigeführt werden. Typischerweise gibt es in Versammlungen folgende Rollen:
- LeiterIn (Sitzungs-/VersammlungsleiterIn) – eine dedizierte Person führt durch die Versammlung, ruft Tagesordnungspunkte auf, erteilt das Rederecht, beendet Diskussionsphasen und führt durch Abstimmungen.
- Protokoll-/SchriftführerIn – eine dedizierte Person protokolliert den Verlauf oder zumindest die Ergebnisse/Beschlüsse der Versammlung.
- TeilnehmerInnen (Mitglieder) – eine klar abgegrenzte Menge an Personen nimmt an der Versammlung teil und kann sich dort durch eigene Diskussionsbeiträge beteiligen. Für Abstimmungen ist zu unterscheiden zwischen
  - den TeilnehmerInnen, die in der Versammlung stimmberechtigt sind, die also an den Abstimmungen teilnehmen dürfen (meist hat jeder stimmberechtigte Teilnehmer eine Stimme, es gibt aber auch Fälle, in denen die TeilnehmerInnen unterschiedliche Stimmgewichte haben) sowie
  - den TeilnehmerInnen, die nicht stimmberechtigt sind.
- Gäste – neben den TeilnehmerInnen kann es auch noch Gäste geben, die per se zunächst kein Rederecht in der Versammlung haben, aber ggf. auf Einladung des Leiters einzelne Redebeiträge ableisten, z. B. in Form von Grußworten, im Rahmen einer Expertenbefragung oder durch einen Gastvortrag.
- ZuschauerInnen – Personen, die der Versammlung in einer in aller Regel rein passiven Rolle folgen.

Den Szenarien liegen zunächst folgende Schutzbedarfe als Annahme zugrunde – evtl. höhere Schutzbedarfe werden im Abschnitt 8 "Bausteine für höheren Schutzbedarf" am Ende des Textes adressiert:

- Verfügbarkeit – normal
- Authentizität – normal
- Integrität – normal
- Vertraulichkeit – normal

Weitere Annahme ist zunächst, dass die Sitzung/Versammlung nicht-öffentlich stattfindet, für die Hinzunahme von öffentlichen ZuschauerInnen/ZuhörerInnen, siehe im Abschnitt 7 Bausteine zur Ergänzung weiterer Funktionalitäten.

5.1 Risiken

Bezogen auf virtuelle Versammlungen sind u. a. folgende Risiken bezogen auf die einzelnen Sicherheitsgrundwerte zu berücksichtigen:

- Verfügbarkeit
  - Ausfall oder Störung der Stromversorgung
  - Ausfall oder technische Störung der Onlineverbindung inkl. des Mobilfunkzugangs, z. B. in Gegenden mit schlechter Netzabdeckung, beim Ausfall von Funkmasten oder durch Überlast
  - Ausfall oder Störung von Dienstleistern
  - Technische Störungen an den Endgeräten
  - Beschädigung, Verlust oder schlichtes Nicht-Mitführen des zur Authentisierung verwendeten Ausweises oder des mobilen Endgeräts
  - DoS/DDoS gegen Videokonferenzsystem
- Authentizität / Integrität
  - Technische Störungen an den Endgeräten
  - Bedienungsfehler des Anwenders
  - Social Engineering, z. B. Phishing von Zugangsdaten zu Videokonferenzen oder zu Administratorenrechten
  - Ungezielte Manipulation des Endgeräts, z. B. Schadsoftwarebefall. Bei der Verwendung eigener Geräte der TeilnehmerInnen (BYOD, bring-your-own-device) kann man sich weder auf Sicherheitsmaßnahmen auf Netzebene noch auf wirksame / homogene Sicherheitsmechanismen der BYOD-Geräte verlassen.
- Vertraulichkeit
  - Mithören/-sehen der Sitzung/Versammlung durch nicht berechtigte TeilnehmerInnen
  - Einsichtnahme in interne Sitzungsunterlagen durch nicht Berechtigte

Die im IT-Grundschutz-Kompendium[11] genannten Gefährdungen gelten grundsätzlich auch für Videokonferenzsysteme.

5.2 Szenario "klein" – Sitzung mit wenigen TeilnehmerInnen

Im Vorfeld der Sitzung haben allen TeilnehmerInnen und ggf. externe Gäste über eine Einladungs-E-Mail die Tagesordnung und Sitzungsunterlagen sowie die personalisierten Zugangsinformationen erhalten. Sie können sich somit zum Sitzungstermin per Desktop-PC, Laptop, Smartphone oder Tablet über einen Link (Meeting URL) in ein Videokonferenzsystem einwählen. Genutzt werden können hierzu Plattformen professioneller Dienstleister (Einladungs- und Anmeldemanagementsystem) oder auf einem eigenen Server installierte Online-Videokonferenzsysteme. Voraussetzung ist, dass die für die Teilnahme an der Versammlung genutzten Geräte über Kamera, Mikrofon und Lautsprecher (oder Headset) und entsprechende Software sowie über eine stabile Internetverbindung verfügen.

Mit angenommenen 10 bis 12 Personen handelt es sich um einen überschaubaren Teilnehmerkreis. Womöglich kennen sich die TeilnehmerInnen bereits oder zumindest der Sitzungsleitung sind die TeilnehmerInnen persönlich bekannt. Die Sitzungsleitung, die über fachliche Adminstratorenrechte verfügt, erkennt die sich einwählenden TeilnehmerInnen auf dem Bildschirm des jeweils genutzten Geräts (Einwahl in das Meeting und Erkennen durch Sitzungsleitung entspricht einer

11 https://www.bsi.bund.de/IT-Grundschutz

"Zweifaktorauthentifizierung") und hat die Möglichkeit, die Einwahl von Unbefugten zu unterbinden. Die Sitzungsleitung verfügt über einen ausreichend großen Bildschirm, etwa einen Großbildschirm für Videokonferenzen, um so einen guten Überblick über alle SitzungsteilnehmerInnen zu behalten. Alle eingewählten Personen können auf den Bildschirmen der TeilnehmerInnen angezeigt werden. Neben den Gesichtern der TeilnehmerInnen kann auf den Displays ein Menü mit weiteren Funktionen angezeigt werden (siehe Bausteine zur Ergänzung weiterer Funktionalitäten).

Die Sitzungsleitung moderiert die Veranstaltung. Sie eröffnet und beendet die Versammlung, Diskussionen, Aussprachen und Abstimmungen, ruft die einzelnen Tagesordnungspunkte auf, verkündet Abstimmungsergebnisse oder kann die Versammlung unterbrechen. Sie sorgt für einen reibungslosen Sitzungsverlauf, gibt Regeln für eine geordnete Diskussion vor, achtet auf die Einhaltung von Redezeiten und erteilt oder ggf. entzieht den RednerInnen das Wort. Sie kann externe Gäste, z. B. Vortragende, für die gesamte Sitzung oder einzelne Tagesordnungspunkte in der Videokonferenz mit Bild oder nur telefonisch hinzuschalten oder deren Einwahl prüfen. Es gibt für Gäste zudem die Option zur Vorstellung von Präsentationen. Zur Wahrnehmung dieser Aufgaben verfügt die Sitzungsleitung über umfangreiche fachliche Administratorenrechte. Aufgrund der überschaubaren Größe der Gruppe ist es für die Sitzungsleitung recht einfach, die Sitzung jederzeit vollständig im Blick zu behalten.

In einem Bereich der Videokonferenzanwendung oder in einer separaten Anwendung mit passwortgeschütztem Zugang können der kleinen Gruppe Dokumente bereitgestellt und von ihr bearbeitet werden (siehe Abschnitt 7.3 Bereitstellung von Dokumenten / Kollaborationen).

Für alle Szenarien gilt: Den Überblick zu bewahren, stellt eine große Herausforderung dar angesichts der Vielzahl nutzbarer Funktionalitäten, etwa das Mitverfolgen der Live-Debatte, die Mitarbeit an Dokumenten und die Kommunikation mit anderen TeilnehmerInnen über mögliche Seitenkanäle - gleichzeitig und über einen einzigen Bildschirm (womöglich auf dem kleinen Display eines Mobile Device).

5.3 Szenario "mittel" – Sitzung/Versammlung mit bis zu 50 Personen

Eine virtuelle Sitzung/Versammlung mit bis zu 50 Personen stellt - aufbauend und ergänzend zum Szenario "klein" - für die Sitzungsleitung eine größere Herausforderung dar. Womöglich sind der Sitzungsleitung nicht alle TeilnehmerInnen bekannt, was im Falle einer visuellen (Zweit)Authentifizierung von Bedeutung sein könnte. Im Vorfeld der Sitzung haben alle TeilnehmerInnen und ggf. externe Gäste über eine Einladungs-E-Mail die Tagesordnung und Sitzungsunterlagen sowie die individuellen Zugangsinformationen erhalten und können sich zum Sitzungstermin per Desktop-PC, Laptop, Smartphone oder Tablet über einen Link (Meeting URL) in ein Videokonferenzsystem einwählen. Dies kann über die Nutzung von Plattformen professioneller Dienstleister oder über die Installation eines kompletten Online-Videokonferenzsystems auf einem eigenen Server erfolgen. Für die Authentisierung denkbar wäre ferner die Akkreditierung in einem "virtuellen Anmelderaum" mit Name, evtl. vorhandener Mitgliedsnummer und vorab individuell zugesandter Akkreditierungsnummer.

Bei der Anzeige von mehreren Dutzend TeilnehmerInnen auf einem Display stellt sich zunehmend die Frage der Übersichtlichkeit. Für die Sitzungsleitung erscheint der Einsatz eines ausreichend großen Bildschirms geboten, um die TeilnehmerInnen im Blick behalten zu können.

Die TeilnehmerInnen sollten die Möglichkeit haben, sich jederzeit zu Wort zu melden und ihre Meinung kundzutun - auch mit Zwischenrufen. Um jedoch eine geordnete Diskussion in einem solchen Größenrahmen sicherzustellen und den Überblick zu behalten, empfiehlt es sich, Redebeiträge bei der Sitzungsleitung anzumelden. Dies könnte über ein eigenes Menü mit Meldefunktion (per Knopfdruck) erfolgen. Die Sitzungsleitung registriert die Meldungen in der Reihenfolge des Eingangs und erteilt den RednerInnen für ihre Beiträge das Wort. Aufgrund der fachlichen Administratorenrechte hat sie die Möglichkeit, nach eigenem Ermessen bzw. gemäß der grundsätzlichen Regeln der Versammlung die Reihenfolge zu ändern und Priorisierungen vorzunehmen. Die Wortmeldungen (Videoaufnahme/Foto, Name und Amt/Funktion der Person) können auf den Displays der TeilnehmerInnen angezeigt werden. Bekommt einer der Fragenden das Wort erteilt, wird dessen Mikrofon laut geschaltet, der nun Sprechende wird allen TeilnehmerInnen auch im Video angezeigt und der Redebeitrag ist für alle hörbar.

Die fachlichen Administratorenrechte der Sitzungsleitung könnten ggf. auch gruppenweise oder generell anwendbar sein (z. B. stumm schalten). Orientiert an Gruppenbildung oder gemeinsamem Abstimmverhalten im realen Leben könnten TeilnehmerInnen sich in virtuelle Gruppe zusammentun, etwa um Teildebatten zu führen oder gemeinsam abzustimmen.

Zur Betreuung einer Veranstaltung dieser Größenordnung ist die Unterstützung der Sitzungsleitung durch weiteres Personal empfehlenswert.

5.4 Szenario "groß" – Versammlung mit vielen Personen

Viele der obigen Ausführungen dürften auch für das Szenario "groß" Gültigkeit behalten. Die Leitung einer virtuellen Sitzung mit mehreren Hundert Personen stellt jedoch eine noch größere Herausforderung dar. So ist beispielsweise eine rein visuelle Authentifizierung durch die Versammlungsleitung nach erfolgter Einwahl ins Online-Videokonferenzsystem nicht möglich oder zumindest unpraktikabel. Zu berücksichtigen sind dabei auch höchstwahrscheinlich vorkommende Verbindungsabbrüche oder Neueinwahlen von TeilnehmerInnen während einer Sitzung. Eine elektronisch unterstützte Authentifizierung erscheint daher dringend geboten. Während bei der Anmeldung für eine kleine Versammlung ein einfaches Anmeldungsprozedere genügen könnte, ist bei einem Großszenario der Einsatz eines professionellen Einladungs- und Anmeldemanagementsystems, am besten mit Mehrfaktor-Authentifizierung, dringend geboten.

Große Versammlungen stellen höhere Anforderungen an die Moderation (Strukturierung der Wortbeiträge) und erfordern straffere Regeln bei der Diskussionen. Eine Gesamtdarstellung bei der Versammlungsleitung auf einem Großbildschirm, der die reale Veranstaltungssituation nachbildet, kann über Großbildschirme bereitgestellt werden. Zur konkreten Steuerung der Versammlung sind darüber hinaus jedoch weitere Sichten auf die Versammlung erforderlich. Eine Unterstützung der Versammlungsleitung durch mehrere Personen ist dabei zu empfehlen.

Die gleichzeitige Abbildung sämtlicher TeilnehmerInnen auf den Displays der durch die TeilnehmerInnen verwendeten Endgeräte ist nicht möglich. Es sollten daher idealerweise mehrere Videokanäle mit unterschiedlichen Bildern zur Auswahl durch die TeilnehmerInnen zur Verfügung gestellt werden. Die Aufrechterhaltung der Übersichtlichkeit angesichts der Vielzahl nutzbarer Funktionalitäten, etwa das Mitverfolgen der Live-Debatte, die Mitarbeit an Dokumenten und die Kommunikation mit anderen TeilnehmerInnen über mögliche Seitenkanäle - gleichzeitig und über einen einzigen Bildschirm (womöglich auf dem kleinen Display eines Mobile Device) - führt zu hoher Komplexität und stellt für die TeilnehmerInnen eine große Herausforderung dar. Um die TeilnehmerInnen zu entlasten, gibt es einen Videokanal mit einem sinnvoll geschnittenen Hauptbild, das alle wesentlichen Beiträge präsentiert.

Zur Betreuung einer Veranstaltung dieser Größenordnung ist aufgrund der damit verbundenen (zusätzlichen) technischen Herausforderungen die Unterstützung durch IT-Personal erforderlich.

5.5 Schutzmaßnahmen

Bei der Konzeption einer virtuellen Versammlung müssen die Fragen der Informationssicherheit von Anfang an mit berücksichtigt werden. Sie sollten in einem Sicherheitskonzept schriftlich niedergelegt werden. Der IT-Grundschutz des BSI bietet hierfür einen breiten Fundus an Anforderungen und – in den Umsetzungshinweisen – konkrete Maßnahme-Empfehlungen. Nachfolgend sollen exemplarisch einige für virtuelle Versammlungen besonders relevante Punkte benannt werden. In vorangestellten Klammern ist bei den Maßnahmen ggf. angegeben, für welche Szenarien (klein, mittel, groß) sie als notwendig angesehen werden.

5.5.1 Grundsätzlich

Bei der Auswahl eines IT-Produkts für Videokonferenzen sollten aus Informationssicherheitssicht folgende Faktoren berücksichtigt werden:

- Geeignete Authentisierungsmechanismen (ggf. Multi-Faktor-Authentisierung)
- Möglichkeiten zu Gruppenmanagement und Zutrittskontrolle
- Umsetzung einer geeigneten Verschlüsselung, ggf. Ende-zu-Ende Verschlüsselung
- Möglichkeit, die Lösung auf einem eigenen Server ("on premise") zu betreiben. Sofern ein eigener Server eingesetzt wird, sollte dieser gehärtet sein, z. B. indem nicht benötigte Funktionalitäten, Schnittstellen und Software ausgeschaltet bzw. entfernt werden.
- Auditierung durch unabhängige Stellen
- Einhaltung der datenschutzrechtlichen Anforderungen

Weiterführende Informationen zu den sicherheitsrelevanten Auswahlkritieren können dem BSI-Kompendium Videokonferenzsysteme[12] entnommen werden.

5.5.2 Verfügbarkeit

- Redundante IT-Ausstattung der Sitzungsleitung (hot standby)
- Zusätzliche Einwahlmöglichkeit per Telefon für die TeilnehmerInnen
- (mittel, groß) Redundante Anbindung der Sitzungsleitung an die zentralen Server
- (groß) Notstromversorgung der zentralen Komponenten der Sitzungsleitung
- (mittel) Verfügbare Unterstützung zur Bedienung der IT
- (groß) Verfügbares Personal für IT-Support
- (mittel/groß) Standard-Maßnahmen gegen DDoS-Angriffe auf Infrastruktur

5.5.3 Authentizität

Ergänzend zu den Ausführungen im Abschnitt 4.3 Authentifizierung seien exemplarisch folgende Punkte benannt:

- Vorgabe an alle TeilnehmerInnen, dass eine Einwahl in die Videokonferenz nur mit Geräten erlaubt ist, die einen aktuellen Patch-Stand vorweisen
- Einwahl in die Videokonferenz zugangsgeschützt, zumindest über Zugangsnummer und ein hinreichend sicheres Passwort, die nur den berechtigten TeilnehmerInnen zur Verfügung gestellt werden
- Sicherstellen, dass auch bei telefonischer Einwahl eine Verbindung zur Konferenz nur mit Zugangsnummer und Passwort möglich ist
- (mittel, groß) Anmeldung der Sitzungsleitung am System per Mehrfaktor-Authentisierung, um fachliche Administrationsrechte zu erlangen
- (groß) Wichtige Redner sollten sich per Mehrfaktor-Authentifizierung am System anmelden.

12 https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Cyber-Sicherheit/Themen/Kompendium-Videokonferenzsysteme.html

5.5.4 Integrität

- (groß) Sichere Verbindung zwischen mobilem Endgerät, zumindest der wichtigen Redner, und zentralem Server über ein Virtuelles Privates Netzwerk (VPN) mit geeigneter Authentisierung des beim zentralen Server registrierten Geräts
- Streaming der Versammlung im Internet zur Herstellung von Transparenz während einer Online-Versammlung, um eventuelle Manipulationen direkt sichtbar zu machen

5.5.5 Vertraulichkeit

- Vorgabe an alle TeilnehmerInnen, inwiefern die Informationen aus der Sitzung/Versammlung vertraulich zu behandeln sind und ob Dritte während der Sitzung/Versammlung mithören dürfen zur Umsetzung durch die TeilnehmerInnen

6 Szenarien für virtuelle Abstimmungen

Für Abstimmungen stehen verschiedene Möglichkeiten zur Verfügung, die mit den zuvor beschriebenen Versammlungsszenarien kombiniert werden können. Nachfolgend skizzieren wir einige dieser Möglichkeiten, durch die eine gemeinsame Willensbildung mithilfe einer Abstimmung erreicht werden kann. Bei offenen Abstimmungen im Rahmen kleiner Sitzungen werden vermutlich Handzeichen im Rahmen der etablierten Videokonferenz ausreichen. Eine technisch unterstützte virtuelle Abstimmung ist hingegen insbesondere in größeren Versammlungen empfehlenswert. Hierzu beschreiben wir verschiedene Ansätze. Wichtig für die Auswahl ist einerseits die Frage nach den funktionalen und den Sicherheitsanforderungen im konkreten Anwendungsfall und andererseits der unterschiedliche Aufwand zur Umsetzung der Varianten.

In dem vorliegenden Text gehen wir nicht auf geheime Abstimmungen ein. Auch hierzu können pragmatische bis technisch sehr versierte Ansätze verfolgt werden, wie in den nachfolgenden Szenarien ausgeführt.

6.1 Risiken

Ergänzend zu den zuvor benannten Risiken bei einer virtuellen Versammlung sind bezogen auf eine virtuelle Abstimmung u. a. noch folgende Risiken zu berücksichtigen.

- Verfügbarkeit
  - Technische Störung der App/Abstimmungswebseite/Wahlsoftware
  - Verzögerung oder erhebliche Beeinträchtigung der Übermittlung der Abstimmung an Server
  - DoS/DDoS gegen Server, der die Abstimmung als Webseite oder für die App bereitstellt, mit der Folge (z. B.)
    - Nichtzählen einer beabsichtigten Stimmabgabe,
    - aber auch Möglichkeit eines Teilnehmers zu behaupten, dass die eigene(n) Stimme(n) nicht gezählt worden ist.
  - DoS/DDoS gegen Webseite, die Abstimmungsergebnis veröffentlicht
- Authentizität / Integrität
  - Mehrfachabstimmungen
  - Abstimmung durch Dritte am Ort des Teilnehmers
  - Manipulation der Stimmauswertung, z. B. durch eingeschleuste Schadsoftware auf Abstimmserver
  - Manipulation der Stimmabgabe, z. B. durch Angriff mit Schadsoftware etc. auf mobile Endgeräte
  - Phishing bzgl. Zugangsdaten für Abstimmungen
  - Manipulation des veröffentlichten Abstimmungsergebnisses, z. B. durch eingeschleuste Schadsoftware auf Webseite, die Abstimmungsergebnis veröffentlicht
- Vertraulichkeit
  - keine
- Sonstige Risiken
  - Unklarheit über Mehrheitsverhältnisse: Bei Abstimmungen in physischen Versammlungen sind Mehrheitsverhältnisse oft näherungsweise erkennbar. Bei einer virtuellen Abstimmung können

sich Mehrheitsverhältnisse auch ad hoc und unerwartet ändern, bspw. durch TeilnehmerInnen, die bei der vorangehenden Debatte noch abwesend waren.

6.2 Szenario "light" – Abstimmung durch Handheben

Variante 1 (wenige Personen): Wenn alle TeilnehmerInnen einer Sitzung in einer gemeinsamen Videokonferenz verbunden sind und (zumindest die Sitzungsleitung) alle TeilnehmerInnen gleichzeitig sieht, kann eine Abstimmung einfach per Handzeichen erfolgen. Die Sitzungsleitung zählt die Stimmen und gibt das Ergebnis bekannt. Voraussetzung ist, dass alle TeilnehmerInnen alle anderen (und deren Abstimmverhalten) sehen können (ggf. durch Durchklicken). Das Szenario eignet sich insbesondere für kleinere Sitzungen.

Variante 2 (wenige Neigungsgruppen, überschaubare Zahl an Personen pro Gruppe): Wenn gruppenweise abgestimmt oder in der Regel einer Empfehlung gefolgt wird, werden die einzelnen Gruppen in einer gemeinsamen Videokonferenz abgefragt. Abweichendes Stimmverhalten könnte zuvor schriftlich mitgeteilt werden und müsste nicht eigens in einem Online-Abstimmungssystem erfasst werden. Es wird durch den "Sprecher" der Gruppe in der Sitzung mitgeteilt.

6.3 Szenario "E-Mail" – Abstimmung per E-Mail

E-Mails mit Voten werden durch die TeilnehmerInnen an die Sitzungsleitung geschickt, oder Voten werden durch die TeilnehmerInnen eigenständig in ein durch die Sitzungsleitung online zur Verfügung gestelltes Dokument eingetragen. Dies ist eine sehr pragmatische Lösung, insbesondere für Abstimmungen, deren Ergebnis nicht sofort vorliegen muss, sowie für nicht kontroverse Abstimmungsgegenstände.

6.4 Szenario "Browser" – Abstimmung in Browser-Anwendung mit transparenter Abstimm-Anzeige

Alle TeilnehmerInnen rufen für die Abstimmung in ihrem Browser eine Webseite auf und authentisieren sich angemessen gegenüber dem Server. Die Sitzungsleitung eröffnet die Abstimmung durch aktives Freischalten einer Abstimmseite auf dem Server. Die TeilnehmerInnen können in ihrem Webbrowser ihr Votum abgeben. Alle Einzelvoten werden in einer großen Übersichtsdarstellung angezeigt, die jede SitzungsteilnehmerIn die ganze Zeit einsehen kann. Nach vorgegebener Zeit endet die Abstimmung.

Aufgrund der Verwendung der Standard-Browser-Technologie ist die Nutzung auf beliebigen Plattformen vereinfacht.

Aufgrund der transparenten Anzeige des Abstimmverhaltens aller TeilnehmerInnen fallen Angriffe (Manipulation der Stimmabgabe) unmittelbar auf. Die Anforderungen an die vorgeschaltete Authentisierung sind daher reduziert.

Der Vorteil der transparenten Anzeige ist, dass eventuelle Manipulationen für den Abstimmenden sofort ersichtlich sind. Sofern zusätzlich ein weiterer Kommunikationskanal zur Sitzungsleitung etabliert würde, eine Art Notfallknopf, um eine Nicht-Übereinstimmung der Anzeige mit der getätigten Abstimmung anzuzeigen, könnte das System als hinreichend manipulationssicher angesehen werden.

6.5 Szenario "App" – Umsetzung über Abstimm-App mit transparenter Abstimm-Anzeige

Alle TeilnehmerInnen nutzen eine für den Abstimmzweck erstellte App auf ihrem Endgerät, die für alle gängigen Plattformen bereitstehen müsste. Die Sitzungsleitung eröffnet die Abstimmung durch aktive Handlung in der App. Die TeilnehmerInnen können in der App nach angemessener Authentisierung teilnehmen und ihr Votum abgeben. Alle Einzelvoten werden in einer großen Übersichtsdarstellung

angezeigt, die jede SitzungsteilnehmerIn die ganze Zeit einsehen kann. Nach vorgegebener Zeit endet die Abstimmung.

Die Umsetzung ist aufwändiger als im vorherigen Beispiel, da die App für jede zu nutzende Plattform (insbesondere Android und iOS für Mobilgeräte, aber auch Windows und Linux für PCs/Notebooks) separat bereitgestellt, gehärtet und getestet werden muss.

Die im vorherigen Abschnitt dargestellten Vorteile der transparenten Anzeige bestehen auch hier.

Es gibt auch Video- oder Audiokonferenzsysteme, bei denen die TeilnehmerInnen für eine Abstimmung nach erfolgter Authentisierung und nach Eröffnung des Abstimmungsprozesses durch die Sitzungsleitung, virtuelle Räume betreten und dadurch ihr jeweiliges Votum abgeben. Die Teilnehmerzahl eines virtuellen Raumes spiegelt die dortige Stimmenzahl wieder. Das Abstimmungsergebnis stünde rasch zur Verfügung und wäre für alle TeilnehmerInnen sichtbar.

6.6 Schutzmaßnahmen

Ergänzend zu den Schutzmaßnahmen bei Versammlungen sollten für den Vorgang der Abstimmungen noch folgende Schutzmaßnahmen umgesetzt werden. Erneut ist in vorangestellten Klammern bei den Maßnahmen ggf. angegeben, für welche Szenarien sie als notwendig angesehen werden.

6.6.1 Grundsätzliches

- Härtung der für die Abstimmung genutzten Server
- (App) Eine einzusetzende App muss gehärtet und vorab auf Sicherheitslücken untersucht werden. Sie sollte zudem zentral verwaltet sein, um sicherstellen zu können, dass nur der Einsatz der aktuellen Version möglich ist.
- (Browser, App) Bzgl. der programmtechnischen Umsetzung der Stimmabgabe ist vorab festzulegen, ob eine Plausibilitätsprüfung bei der Stimmabgabe stattfinden soll. Damit wären ungültige Stimmen nur möglich, wenn die Option "ungültig" mit zur Auswahl gestellt wird.
- (E-Mail, Browser, App) Mit Unterbrechung einer Debatte und Beginn einer Abstimmung könnte die Versammlungsleitung die Stimmberechtigten feststellen und die Einwahl für bisher nicht teilnehmende Personen sperren.

6.6.2 Verfügbarkeit

- (ist bei den Szenarien E-Mail, Browser, App implizit umgesetzt) Redundante Anbindung der TeilnehmerInnen (z. B. ein Kanal für die Sitzungsteilnahme, ein Kanal für die Abstimmung)
- (Browser, App) Notfallknopf / -kanal, um Fehlverhalten des Systems (es werden Stimmabgaben falsch angezeigt oder abgegebene Stimmen werden als "noch nicht abgegeben" angezeigt) jederzeit anzeigen zu können und somit die Feststellung des Abstimmungsergebnisses legitim zu verzögern
- (Browser, App) Verfügbarkeit einer schnell verfügbaren Ersatzlösung für TeilnehmerInnen, um Teilnahme an Abstimmungen zu ermöglichen, für den Fall von Beschädigung, Verlust oder schlichtem Nicht-Mitführen des zur Authentisierung verwendeten Ausweises oder des mobilen Endgeräts
- (E-Mail, Browser, App) Verfügbarkeit von telefonischen Erreichbarkeitsdaten der TeilnehmerInnen, sodass die Sitzungsleitung Voten, die nicht oder nicht korrekt übermittelt wurden, im Einzelfall händisch erfragen kann (verhindert das absichtliche Blockieren einer Abstimmung wegen "angeblicher" Nicht-Übermittlung eines Votums)
- (E-Mail, Browser, App) Bereithalten (cold standby) einer alternativen Technik für Abstimmungen, falls ein Mechanismus, z. B. aufgrund technischer Störung, nicht zur Verfügung steht

6.6.3 Authentizität

Ergänzend zu den Ausführungen im Abschnitt 4.3 Authentifizierungseien exemplarisch folgende Punkte benannt:

- (E-Mail, Browser, App) Um sicherzustellen, dass nur die TeilnehmerIn persönlich ihre Stimme(n) abgibt, sollte eine neue Authentisierung bei jeder Stimmabgabe erfolgen.
    - (E-Mail) Bei Abstimmungen per E-Mail könnte ein Einmal-Passwort-Mechanismus eingesetzt werden, um sicherzustellen, dass nur Berechtigte abstimmen. Dies ist bei kleinen Sitzungen/Versammlungen nicht erforderlich, sofern davon ausgegangen werden kann, dass alle Stimmberechtigten auch abstimmen.
- (E-Mail, Browser, App) Um sicherzustellen, dass jeder Teilnehmer nur genau die ihm zustehende Stimmenzahl abgeben kann, erfolgt nach der Authentisierung bei einer konkreten Abstimmung ein Abgleich, ob der Teilnehmer bereits abgestimmt hat.

6.6.4 Integrität

- (E-Mail, Browser, App – ist bei "light" implizit) Herstellung von Transparenz während einer Abstimmung, um Manipulationen direkt sichtbar zu machen
- (E-Mail, Browser, App) Notfallknopf für TeilnehmerInnen zum Hinweis auf Abweichung der Anzeige von erfolgter Wahl ermöglicht Korrektur bzw. Angriffserkennung vor Feststellung des Abstimmungsergebnisses durch den Veranstalter oder die einladende Organisation

7 Bausteine zur Ergänzung weiterer Funktionalitäten

7.1 Atmosphäre (Zwischenfragen, Zwischenrufe, Beifall)

Die Atmosphäre einer virtuellen Veranstaltung ist eine andere als in der realen Welt. Virtuelle Veranstaltungen können Präsenzveranstaltungen sicherlich ergänzen, womöglich aber nicht völlig ersetzen, zumindest nicht atmosphärisch. Um dennoch eine hinreichend lebendige Diskussion zu ermöglichen und der Veranstaltung einen möglichst lebendigen Charakter zu verleihen, müssen sich die TeilnehmerInnen live in die Diskussion einschalten und miteinander in Dialog treten können, auch wenn den Sprechenden von der Sitzungsleitung nicht formell das Wort erteilt wird. Auf diese Weise könnten auch kurze Zwischenfragen, Zwischenrufe und Beifall visuell und akustisch wahrgenommen werden. Applaus könnte hierbei auf dem Server künstlich erzeugt werden, ausgelöst durch Klicks der TeilnehmerInnen auf einen Applaus-Knopf und in der Lautstärke abhängig von der Zahl der applaudierenden TeilnehmerInnen. Dadurch könnte zumindest ein Hauch von Präsenzversammlung entstehen. Möchte sich jemand aus dem Teilnehmerkreis nicht beteiligen oder kurz ausklinken, so kann die Person die Stummschalte-Funktion oder "Black-Screen-Funktion" betätigen. RednerInnen können sich durch Handzeichen oder durch Zwischenruf zu Wort melden.

7.1.1 zusätzliche Risiken

- Verfügbarkeit
  - Unabsichtliche Störung: Wenn viele TeilnehmerInnen gleichzeitig ihre Mikrofone geöffnet haben, können Nebengeräusche und Rückkopplungen verhindern, dass der eigentliche Hauptsprecher zu verstehen ist.
  - Absichtliche Störung: Störung des Audio- oder Videokanals durch Demonstration, öffentlichkeitswirksame Aktion etc.
- Vertraulichkeit
  - Wenn TeilnehmerInnen eigenständig ihre Mikrofone öffnen können bzw. eingeschaltet lassen können, besteht die Gefahr, dass Gespräche ungewollt in die Besprechung übertragen werden, weil vergessen wurde, dass das Mikrofon noch offen ist.

7.1.2 Schutzmaßnahmen

- Zwischenfragen oder Beitragswunsch über zweiten Kanal realisieren, um Störgeräusche zu vermeiden und strukturierteren Ablauf zu ermöglichen
- Steuerung der Audio- und Videoübertragung durch Sitzungsleitung, sodass HauptrednerIn im Vordergrund, andere Geräusche im Hintergrund zu hören sind, ggf. getrennte Audio-Kanäle, sodass TeilnehmerInnen und ZuhörerInnen das Lautstärkeverhältnis individuell regulieren können

7.2 Seitenkommunikation einzelner TeilnehmerInnen

Der zwischenmenschliche Aspekt und die Gelegenheit zu zwanglosen, informellen Gesprächen und Gruppenbildungen während oder am Rande von Versammlungen ist von großer Bedeutung. Die Dynamik einer Versammlung entfaltet sich keineswegs nur in den offiziellen Sitzungen der Gremien oder im Plenum. Da SitzungsteilnehmerInnen in der realen Welt die Möglichkeit haben, visuell oder verbal, z. B. durch Zurufe, Dialoge oder Handzeichen, zu zweit oder mit mehreren Personen, innerhalb oder außerhalb des Versammlungsraums direkt miteinander zu kommunizieren und sich abzustimmen, sollte dies auch bei einer virtuellen Versammlung möglich sein. Hierfür sollten innerhalb der Videokonferenzplattform des Veranstalters eigene, von der Sitzungsleitung unabhängige und unbeobachtete Kommunikationskanäle zur

Verfügung gestellt werden, etwa virtuelle (Ad-hoc-)Versammlungsräume mit Video- und Chatfunktionen. Viele Instant-Messaging-Programme bieten diese Funktionalität bereits an.

7.2.1 zusätzliche Risiken

- (Grundsätzlich) Unabhängig von der durch den Veranstalter bereitgestellten IT wäre es den TeilnehmerInnen auch möglich, über alternative bzw. private Chat-Programme / Instant Messenger miteinander zu kommunizieren. Da hierfür vom Veranstalter keinerlei Sicherheitsvorgaben gemacht und umgesetzt werden können, wird hiervon abgeraten.
- (Authentizität/Vertraulichkeit) Seitengespräche dienen häufig auch strategischen Vorabsprachen und finden nur unter Vertrauten statt. Ein unbemerktes Mithören durch Dritte muss verhindert werden.

7.2.2 Schutzmaßnahmen

- (Authentizität/Vertraulichkeit) Alle Anwesenden innerhalb eines ad-hoc nutzbaren Versammlungsraums sollten mit ihren im Rahmen der Authentisierung für die Gesamtversammlung erfassten Namen/Pseudonymen auf den Bildschirmen angezeigt werden.
- (Vertraulichkeit) Die Ad-hoc-Räume könnten "von innen abschließbar" sein, sodass nach Diskussionsbeginn niemand mehr unbemerkt dazustoßen kann.

7.3 Bereitstellung von Dokumenten / Kollaborationen

Die für die Durchführung der Versammlung erforderlichen Dokumente (z. B. Einladungen, Tagesordnungen, Berichte, Präsentationen, Anträge sowie Video-/Tonaufzeichungen und Protokolle zurückliegender Sitzungen) können auf einem Server oder in einer Cloud abgelegt und dort von den TeilnehmerInnen vor, während und nach der Versammlung eingesehen werden. Durch die Versammlungsleitung kann im Rahmen ihrer fachlichen Administratorenrechte den TeilnehmerInnen je nach Amt und Funktion (z. B. Unterscheidung zwischen Vorstandsmitglied oder einfachem Mitglied) oder Gruppenzugehörigkeit Zugang gewährt werden. Je nach Anlass könnte auch externen Personen, wie Gästen oder der Öffentlichkeit, teilweise oder vollumfänglich, ggf. auch mit zeitlicher Verzögerung (z. B. erst nach einer Sitzung) Zugriff ermöglicht werden. Die Authentisierung kann über einen passwortgeschützten Bereich erfolgen, z. B. über die Website des Veranstalters, aus der authentisierten Videokonferenz-Sitzung oder direkt bei einem Cloud-Dienst (Authentisierung mit Name oder Mitgliedsnummer in Verbindung mit einem Passwort).

Virtuelle Versammlungen bieten auch die Möglichkeit der (Live-)Kollaboration: So können die TeilnehmerInnen auf dem Server des Veranstalters gemeinsam an Initiativen oder Anträgen arbeiten, diese kommentieren und sich dazu untereinander abstimmen. Zu diesem Zweck könnte ihnen über ein entsprechendes Menü im Videokonferenzsystem ein umfangreiches Nutzungs-/Beteiligungsangebot bereitstehen, etwa Meeting-Kalender, Planungstools, Wiki, virtuelles Whiteboard (zur direkten Bearbeitung von Dokumenten). Der Bearbeitungsstand von Dokumenten wird allen Berechtigten angezeigt. Hierfür bedarf es entsprechender Softwarelösungen und Lizenzen. Die Sitzungsleitung kann die entsprechenden Zugriffsberechtigungen erteilen (Freischaltung) und kann diese ggf. auch wieder entziehen (Sperrung). Des Weiteren lassen sich nach ähnlichem Muster im internen Bereich Gruppen oder virtuelle Versammlungsräume einrichten, in denen die TeilnehmerInnen je nach Amt, Funktion oder Gruppenzugehörigkeit gemeinsam an Projekten arbeiten, Dokumente ablegen und miteinander kommunizieren können. Weitere Funktionen könnten die direkte Übermittlung von Dokumenten an die Sitzungsleitung umfassen, die einen vollständigen Überblick über alle vorliegenden Dokumente erhält. Die Freischaltung zur Arbeit an Dokumenten kann bereits vor der Versammlung erfolgen. Durch ein solches Prozedere könnte die Abstimmung von Anträgen etc. im Umlaufverfahren (z. B. per E-Mail) überflüssig werden.

In Abgrenzung zu Nebendiskussionen / Seitenkanälen sind in diesem Abschnitt institutionalisierte Formen der Kollaboration und offizielle Gruppen oder Gremien gemeint.

7.3.1 zusätzliche Risiken

- (Verfügbarkeit) DoS auf die Plattform oder Ausfall von Komponenten, z. B. mit dem Ziel der Löschung oder Manipulation der dort liegenden Dokumente
    - Besondere Risiken bzgl. Einhaltung von Fristen etc. (MA: Was heißt das?)
- (Authentizität/Vertraulichkeit) Unautorisierter Zugriff durch
    - Leak der Zugangsdaten
    - Fehlerhafte Zuordnung von Personen zu Gruppen
    - Fehlerhafte Freigabe (Irrläufer)
    - Verlust von "private links", falls vorhanden (Links mit Hash, der direkten Gast-Zugang zu einem Dokument oder einer Kollaborationsoberfläche gibt)
    - Versäumnis, ehemalige Zugriffsrechte wieder zu entziehen
    - Erraten von Links, durch Erkennung des Musters ("sitzung_2020_02_01", "sitzung_2020_03_01", ...). Das Nichtbekanntgeben existierender Links schützt daher nicht immer vor unautorisiertem Zugriff.
    - Einsicht durch den Plattformbetreiber
- Vertraulichkeit
    - durch unautorisierten Zugriff, s.o.
    - Das Risiko des Vertraulichkeitsverlustes steigt mit der Zeit, die ein Dokument verfügbar ist. Mangelnde Übersicht über die Dokumente, die man selber freigegeben hat und freigegeben bekommt, erhöhen das Risiko ebenso, z. B. eine Plattform arbeitet mit einer Zugriffskontrolle, die allein auf Basis des Links erfolgt (wer den Link kennt, kann zugreifen). Gleichzeitig werden Dokumente oftmals nach ihrer Verwendung nicht gelöscht. So sind sie für Dritte dauerhaft einsehbar, wenn sie den Link kennen oder erraten. Es bedarf der Transparenz der Freigaben und Freigabebeziehungen.
    - Versionierung der Dokumente schützt vor Datenverlust. Frühere Versionen und Textbausteine sind damit aber oftmals zeitlich unbegrenzt wiederherstellbar. Hier kann auch ein Vertraulichkeitsverlust (ggü. anderen autorisierten Nutzern) entstehen, wenn der Autor annimmt, eine Äußerung oder Passage aus dem gemeinsamen Dokument eliminiert zu haben.
- Integrität
    - Integritätsverlust kann auch so verstanden werden, dass Nutzer gleichzeitig (offline) an einem Dokument weiterarbeiten und ein Zusammenführen nur schwer möglich ist (Divergenzen in den Versionen). Im schlechtesten Falle löscht einer der Nutzer die Änderungen des anderen beim Aktualisieren des Dokumentes.

7.3.2 Schutzmaßnahmen

- (Grundsätzlich) Schutzmaßnahmen sind hier analog zum Videokonferenzsystem umzusetzen. Wichtig ist hier, ein umfassendes Rollen- und Rechtemanagement zu etablieren. Wenn das System zur Bereitstellung von Dokumenten und zur Kollaboration eng mit dem Videokonferenzsystem verknüpft ist, bietet es sich an, die Authentisierung nur einmalig für beide Systeme durchzuführen.

- Rechtemanagement umfasst hier insbesondere, wie oben beschrieben, den Transparenzgedanken: User müssen zu jeder Zeit in der Lage sein, zu verstehen, welche eigenen Dokumente wem freigegeben worden sind und welche Freigaben man selbst zur Zeit besitzt.
- (Verfügbarkeit) Backup-Konzept für die Unterlagen
- (Integrität)
  - Aktionen wie das Hinzufügen, Löschen und Ändern von Dokumenten müssen protokolliert werden.
  - Änderungen innerhalb von Dokumenten sollten versioniert/protokolliert werden.
  - Synchrone Kollaborationsplattformen ermöglichen ein gleichzeitiges Arbeiten am Dokument, ohne individuelle Kopien erzeugen zu müssen.

7.4 Protokollierung / Dokumentation

Je nach Ausgestaltung einer virtuellen Versammlung (siehe auch 7.1 Atmosphäre (Zwischenfragen, Zwischenrufe, Beifall)) können, durch die Möglichkeit der Aufzeichnung der Veranstaltung, die Dokumentation und die Arbeit der Protokollanten erleichtert, stenografische Mitschriften und klassische Protokollführung damit teilweise sogar überflüssig werden. So könnten knappe Ergebnisprotokolle eventuell ausreichen und zur Verfügung gestellt werden (siehe 7.3 Bereitstellung von Dokumenten / Kollaborationen).

Audio- und Videoaufzeichnungen, Protokolle und Dokumente können im Nachgang auch einem größeren Interessentenkreis und der Öffentlichkeit zur Verfügung gestellt bzw. online abgerufen werden, beispielsweise auf der Website der Veranstalter (z. B. in der Mediathek mit Links zu den entsprechenden Dokumenten, wie Anträgen oder Protokollen). Zusätzlich oder alternativ lassen sich Videoaufzeichnungen auf den gängigen Videoplattformen einstellen.

7.4.1 zusätzliche Risiken

- (Verfügbarkeit) Angriff auf Server oder Cloud mit dem Ziel der Löschung oder Manipulation der Dokumentation (Video-/Tonaufzeichnungen und Dokumente)

7.4.2 Schutzmaßnahmen

- (Verfügbarkeit) Backup-Konzept für die Unterlagen und Video-/Tonbandaufzeichnungen

7.5 Dolmetschen / Gebärdensprache

Bei der Einladung fremdsprachiger TeilnehmerInnen oder Gäste könnte der Einsatz von Simultan- oder Konsekutiv-DolmetscherInnen erforderlich werden. Entsprechende Serviceleistungen könnten von der Sitzungsleitung zugeschaltet werden oder könnten sich per vorab individuell zugesandtem Einwahlcode (siehe oben bei Szenarien) selbst hinzuschalten. Auch dieser Prozess könnte über eine Mehrfaktorauthentisierung erfolgen (Online-Einwahlprozess und visuelle Erkennung der Eingewählten durch Sitzungsleitung). Es ist davon auszugehen, dass DolmetscherInnen qualitativ höherwertigere Ton- und Videoaufnahmegeräte zur Verfügung stehen müssen als zur bloßen Versammlungsteilnahme erforderlich wären.

Die DolmetscherInnen könnten, sofern gewünscht, wie die TeilnehmerInnen auch, auf den Bildschirmen aller sichtbar sein (Bild- und Tonübertragung). Die TeilnehmerInnen können über ein Funktionsmenü Bild und Ton, nur Bild oder nur Ton, je nach Bedarf und Interesse, ein- oder ausschalten oder auf die Inanspruchnahme des Dolmetscher-Service ganz verzichten. Beim Einsatz von mehrsprachigen Simultan-

oder Konsekutiv-DolmetscherInnen können sie zwischen mehreren Kanälen wechseln. Die Sitzungsleitung verfügt im Rahmen ihrer fachlichen Administratorenrechte über entsprechende Freischaltfunktionen.

Gleiches gilt grundsätzlich auch für den Einsatz von GebärdensprachendolmetscherInnen, damit auch gehörlosen Menschen die Teilnahme an Online-Veranstaltungen ermöglicht und die Kommunikation zwischen ihnen und hörenden Menschen gewährleistet werden kann. Die TeilnehmerInnen haben die Möglichkeit, GebärdensprachendolmetscherInnen je nach Bedarf und Interesse auf ihren Bildschirmen ein- und auszublenden.

Daneben wären weitere Möglichkeiten und technische Lösungen zur Sicherstellung von Barrierefreiheit im virtuellen Raum zu prüfen.

7.5.1 zusätzliche Risiken

keine zusätzlichen

7.5.2 Schutzmaßnahmen

keine zusätzlichen

7.6 Übertragung der Versammlung ins Internet (Öffentlichkeit)

Eine Übertragung von Versammlungen in die Öffentlichkeit (Streaming) wird bereits vielfach praktiziert. Die ZuschauerInnen können der Sitzung live in Bild und Ton folgen. Möglicherweise können zusätzlich barrierefreie Übertragungsformen angeboten werden. So könnten die GebärdensprachendolmetscherInnen auf Wunsch der jeweiligen ZuschauerInnen eingeblendet werden (einstellbar über Menüfunktion).

Im Falle einer Übertragung über die Website / Plattform der Veranstalter: Eine Teilnahmerregistrierung für die Öffentlichkeit könnte angebracht sein, wenn die Möglichkeit zur Beteiligung an Diskussionen besteht. Hier wäre dann eine Online-Anmeldung auf der Übertragungswebsite und Authentisierung erforderlich (ähnlich wie oben bei den Szenarien beschrieben). Die Sitzungsleitung hätte im Rahmen ihrer fachlichen Administratorenrechte die Möglichkeit, Fragewünsche der ZuschauerInnen zu registrieren, ihnen das Wort zu erteilen und zu entziehen bzw. schriftlich, z. B. über eine Chatfunktion, eingereichte Fragen selbst vorzutragen. Je nach Wunsch der Veranstalter wären weitere Formen der Zuschauerbeteiligung möglich, z. B. Kommentierung von Anträgen oder Einbringung eigener Vorschläge in den Diskussionsprozess. Möglich wäre hierzu auch die Einrichtung einer eigenen Online-Beteiligungsplattform.

Viele Veranstaltungen werden bereits über öffentliche Plattformen / Soziale Medien übertragen und bieten - in der Regel registrierten - ZuschauerInnen die Möglichkeit für Diskussionen und Kommentare. Auch hier bestünde seitens der Veranstalter die Möglichkeit der Moderation.

7.6.1 zusätzliche Risiken

- (Verfügbarkeit) Nichtverfügbarkeit des Streams

7.6.2 Schutzmaßnahmen

- Die Übertragung (Streaming) sollte aus informationssicherheitstechnischer Sicht getrennt werden vom internen System, über das die Versammlung durchgeführt wird. Es sollte über leistungsstarke Anbieter, die auch mit Lastspitzen umgehen können, angeboten werden.
- Redundanz der Anbindung des Streaminganbieters an die Stream-Produktion der Versammlung

7.7 Geheime Abstimmung

Der Aspekt der geheimen Abstimmung ist nicht Teil dieser Veröffentlichung. Siehe hierzu die gesonderte Publikation auf den BSI-Webseiten zum Thema[13].

13 https://www.bsi.bund.de/viva

8 Bausteine für höheren Schutzbedarf

Für Situationen, in denen bzgl. einzelner Sicherheitsgrundwerte erhöhte Anforderungen bestehen, werden im Folgenden einzelne relevante Risiken und Schutzmaßnahmen aufgeführt, die zusätzlich zu den zuvor genannten zu betrachten sind. Wichtig ist jedoch, dass bzgl. hoher Risiken eine ergänzende Risikoanalyse durchzuführen ist. Nur so kann sichergestellt werden, dass den spezifischen Begebenheiten angesichts des besonderen Schutzbedarfs ausreichend Rechnung getragen wird.

8.1 Schutzbedarf hoch bzgl. Verfügbarkeit

Für besonders hohe Anforderungen an die Verfügbarkeit hat das BSI eine Reihe von Dokumenten zum Thema Hochverfügbarkeit/Rechenzentrum-Sicherheit[14] veröffentlicht, dem Ansätze und Ideen zur Umsetzung weiterer Maßnahmen entnommen werden können.

8.1.1 zusätzlich adressierte Risiken

- Gezielte Angriffe auf die Verfügbarkeit der für die Versammlung und Abstimmungen genutzten zentralen IT-Infrastruktur inkl. deren Anbindung an das Internet
- Gezielte Angriffe auf die IT einzelner TeilnehmerInnen oder die Internetverbindung zwischen TeilnehmerInnen und Veranstalter

8.1.2 Schutzmaßnahmen

- Vorsorgliche Kooperation mit DDoS-Mitigation-Anbietern, um Angriffe kurzfristig "abwehren" zu können
- Umsetzung der Versammlung in einem eigenen, vom Internet separierten Netz

8.2 Schutzbedarf hoch bzgl. Authentizität

8.2.1 zusätzlich adressierte Risiken

- Angriffe auf / Umgehen von einfache(n), z. B. passwortgestützte(n), Authentisierungsmechanismen
- Gezielte Manipulation von Endgeräten

8.2.2 Schutzmaßnahmen

- Wenn eine technisch sichere Authentisierung genutzt werden soll, so gilt es, einen Mechanismus nach TR 3107[15] auszuwählen, der für des Vertrauensniveau hoch geprüft ist. Darauf aufbauend können durch das BSI bewertete Verfahren ausgewählt und eingesetzt werden.

  Ein mögliches Modell wäre die Nutzung des Personalausweises als externes Sicherheitstoken oder das Ausrollen von sicheren Chipkarten. Im konkreten Anwendungsfall kann man auch eigene Authentifizierungsmittel ausgeben, die die TeilnehmerInnen mit nach Hause nehmen können, z. B. könnte man die Technologie des Personalausweises auf Dienst- oder Mitgliederausweise übertragen. Dies hätte den Vorteil, dass die benötigten Sicherheitskomponenten schon verfügbar und direkt in ein Videokonferenzsystem und eine Abstimmungs-App integrierbar wären.

14 https://www.bsi.bund.de/DE/Themen/Unternehmen-und-Organisationen/Informationen-und-Empfehlungen/Empfehlungen-nach-Angriffszielen/Hochverfuegbarkeit/hochverfuegbarkeit.html
15 https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Publikationen/TechnischeRichtlinien/TR03107/TR-03107-1.html

Die Authentisierungsfunktion des Personalausweises kann auch in Kombination mit dem Mobiltelefon (statt eines separaten Kartenlesers) genutzt werden, sodass hier eine praktikable Lösung zur Verfügung steht.

- Einsatz begrenzen auf von der Organisation des Veranstalters ausgegebene und administrierte Endgeräte (Mobile Device Management), also kein Einsatz von Bring-your-own-device-Geräten.

8.3 Schutzbedarf hoch bzgl. Integrität

8.3.1 zusätzlich adressierte Risiken

- Gezielte Manipulation der Beiträge einzelner TeilnehmerInnen
- Gezielte Manipulation der Verdolmetschung / Gebärdensprache
- Angriff auf die Gerätehardware bei physischem Zugriff. Dies würde stets auch vollen Zugriff auf das Betriebssystem, die Dienste und Anwendungen bedeuten.
- Manipulation von Schlüsselpersonen (Funktionsposten) durch Social Engineering
- Morphing
- Deep Fakes

8.3.2 Schutzmaßnahmen

- Die Übertragung zwischen IT-System und Videokonferenz muss integritätsgeschützt sein.
- Zum Schutz vor Geräte-Manipulation ist der Einsatz zentral gemanagter Endgeräte zu empfehlen: Es sollten ausschließlich die von der Organisation des Veranstalters zentral verwalteten Mobilgeräte eingesetzt werden. Dies vereinfacht auch die Erstellung / Programmierung / Pflege der eingesetzten Videokonferenzlösung und Abstimm-App und sogar deren Nutzung, weil die eingesetzten Endgeräte dann sicher und zuverlässig funktionieren. Wenn alle Mobilgeräte über ein zentrales Mobile Device Management (MDM) abgesichert werden, ergibt sich in Bezug auf alle Sicherheitsziele ein Sicherheitsgewinn.
- Durch ein Rechte- und Rollenkonzept muss für Administrationsrollen ein 4-Augen-Prinzip umgesetzt werden.

8.4 Schutzbedarf hoch bzgl. Vertraulichkeit

Es bestehen besondere Anforderungen an die Vertraulichkeit der Inhalte. Dies erfordert zwingend auch einen hohen Schutzbedarf bzgl. Authentizität der TeilnehmerInnen. Insofern sind o. g. Maßnahmen umzusetzen.

Aspekte einer geheimen Abstimmung werden in dieser Veröffentlichung nicht adressiert, siehe hierzu BSI-Webseiten[16].

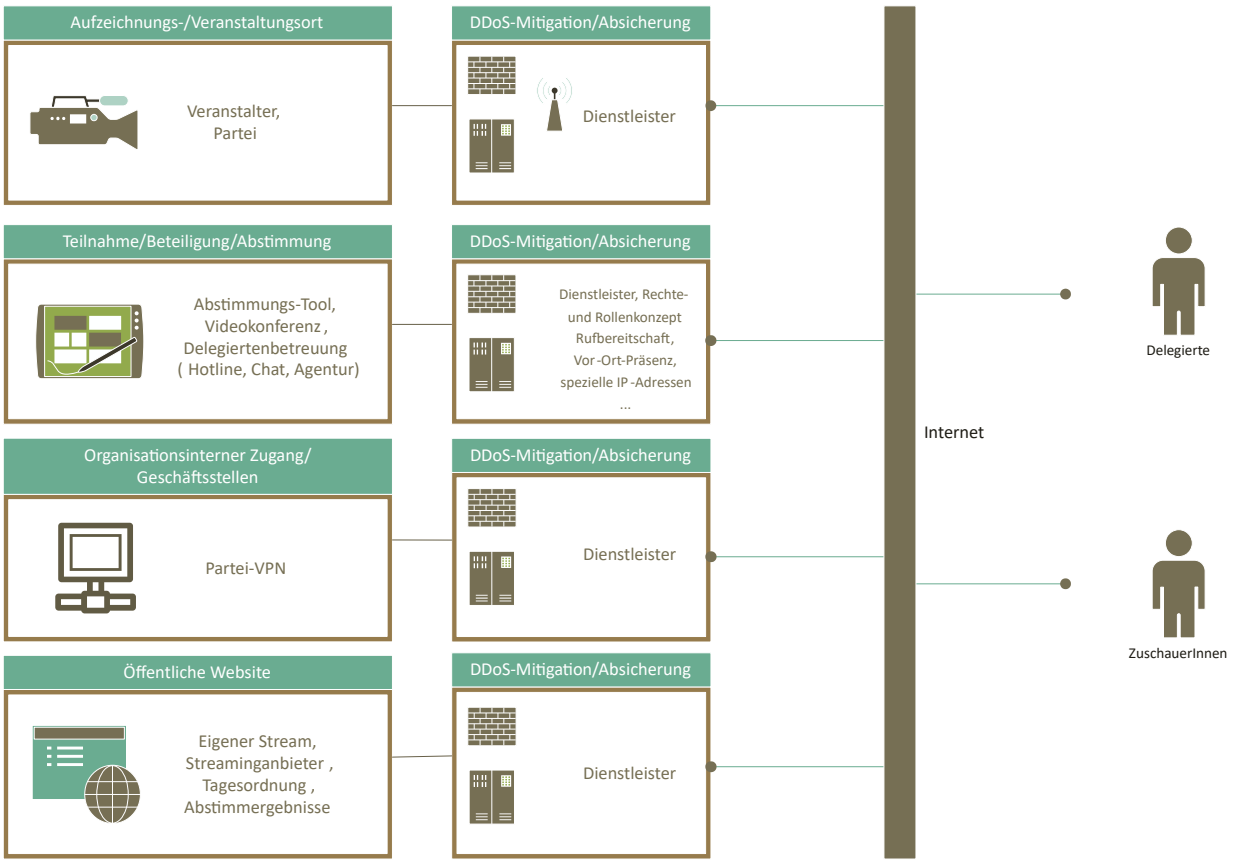
16 https://www.bsi.bund.de/viva

9 Praxisbeispiel Parteitage

Herausgehobene Veranstaltungen wie Parteitage verbinden viele der zuvor genannten Handlungsempfehlungen und Best-Practice-Beispiele virtueller Versammlungen und Abstimmungen. Zugleich ergeben sich besondere Herausforderungen für eine sichere Gestaltung. So ist der politische Fokus der Veranstaltung nicht nur inhaltlich zu sehen, sondern auch bezogen auf politisch motivierte Angriffsversuche und politische Folgen zu berücksichtigen. Nicht selten fällt somit das Ziel der technischen Resilienz zusammen mit dem Ziel der demokratischen Resilienz.

Ergänzend zu den zuvor beschriebenen Versammlungs- und Abstimmungsszenarien und zusätzlichen Bausteinen bedeuten Parteitage organisatorisch u. a. wechselnde oder veränderbare Tagesordnungen, Interaktionsmöglichkeiten durch Delegierte und Gäste, heterogene Endgeräte sowie eine umfangreiche Netzwerkinfrastruktur und Systemlandschaft, die ggfs. wiederum viele Dienstleistungsunternehmen und „Gewerke“ erfordern. Parteitage stehen zudem im Fokus von Öffentlichkeit und Presse, was die Vorbereitung einer Vorfalls- bzw. Krisenkommunikation unabdingbar macht. Auch ist in Zukunft weiterhin mit einem Bedarf an digitalen Hybridveranstaltungen zu rechnen, um sowohl eine Präsenz vor Ort als auch eine virtuelle Beteiligung zu ermöglichen, was die Angriffsfläche weiter vergrößert (mehr Netz- und Systemkomponenten, weitgehend offener Veranstaltungsort, externe Gäste usw.).

Beispiel einer Netzwerkinfrastruktur und Systemlandschaft:



9.1 zusätzliche Risiken

- (Verfügbarkeit) DoS auf die Systeme oder Ausfall von Komponenten/Diensten
- (Verfügbarkeit) Nichtverfügbarkeit des Streams
- (Verfügbarkeit) Technische Probleme bei Beteiligung von Delegierten, z. B. Ton-Ausfall, Probleme bei Stimmabgabe
- (Authentizität / Vertraulichkeit) Social Engineering, unautorisierter Zugriff auf Versammlung und/oder Abstimmungen
- (Authentizität / Vertraulichkeit) Missbrauch von Berechtigungen
- (Authentizität / Vertraulichkeit/Verfügbarkeit) Wiederholte Fake-Einträge/-Anmeldungen in Registrierungs-, Anmelde- oder Eingabefeldern von Websites
- (Authentizität / Vertraulichkeit) Diebstahl und Manipulation von Geräten, Datenträgern oder Dokumenten

9.2 Schutzmaßnahmen

- Grundsätzlich
  - Risikoanalyse und Sicherheitskonzeption
    - Übersicht über Gesamtinfrastruktur nötig (von Firewall bis Konfiguration des Webservers) und Koordination der IT
    - Erstellung einer Risikoanalyse
  - Notfallmanagement und Krisenkommunikation
    - Erreichbarkeiten/Rufbereitschaften sicherstellen (auch Vorbereitung der Kontakte zu Providern/externen Dienstleistern)
    - kontinuierliche Kommunikation aller Beteiligten nötig (z. B. auch zwischen Social-Media-Team und Systemadministratoren)
  - Vorbereitung von Pausen, Videoeinspielern oder Moderation zur Überbrückung von Ausfällen, Notfallreaktionsmaßnahmen (Software-Updates/Deployment) oder Arbeitspausen der IT-Administration
  - Bauliche, organisatorische Schutzmaßnahmen
- Verfügbarkeit
  - erweiterter DdoS-Schutz
    - u. a. Layer-7-DDoS-Schutz „URI Request Limiter inkl. Blacklisting“
  - Redundanz bei Netzzugängen des Veranstaltungsortes (z. B. auch LTE-Backup)
  - Redundanz bei zentralen Systemen und Servern
  - vorbereitete, jederzeit abrufbare DDoS-Mitigation bei Netzknoten/Providern
  - Skalierbarkeit, Caching rechenintensiver und öffentlicher Applikations-Endpunkte
  - Redundanter Administrations-Zugriff auf Server (z. B. dedizierte Leitung oder LTE)
  - Captchas, Rate-Limiting, Geoblocking oder intelligente Client-Fingerprinting-Techniken bei Registrierungs-, Anmelde- oder Eingabefeldern
  - Zugang / Teilnahme für Delegierte ermöglichen:

    - Testläufe
    - Videokonferenz-Proberäume
    - Betreuung, Hotline, Ticketsystem bei technischen Problemen
- Authentizität / Vertraulichkeit
    - Rechte- und Rollenkonzept
    - Entzug von Rollen nach Nutzung
    - 4-Augen-Prinzip/Reviewprozess bei Systemadministration
    - Schulung der Systemadministration
    - Verschlüsselung der Endgeräte der Administratoren, Bildschirmsperre
    - Hardware-Token zur Authentisierung
    - Zugangskontrollen zum Veranstaltungsort
    - Sicherheitsbewusstsein schaffen bei EndnutzerInnen

10 Zusammenfassung und Aufruf zur Kommentierung

Im vorliegenden Papier wird ein Überblick über informationstechnische Herausforderungen und Lösungsansätze bzgl. virtueller Versammlungen und Abstimmungen gegeben. Je nach Größe und Ausgestaltung der Versammlungen stehen unterschiedliche Umsetzungsvarianten zur Verfügung, die durch weitere Elemente (Bausteine) ergänzt werden können.

Zum Themenfeld finden Sie weitere BSI-Publikationen auf den BSI-Webseiten[17].

Darüber hinaus möchten wir auf folgende Veröffentlichung hinweisen:

Council of Europe, Recommendation CM/Rec(2017)5 of the Committee of Ministers to member States on standards for e-voting, 14.06.2017[18], mit Anhängen.

17 https://www.bsi.bund.de/viva
18 https://www.coe.int/en/web/electoral-assistance/e-voting