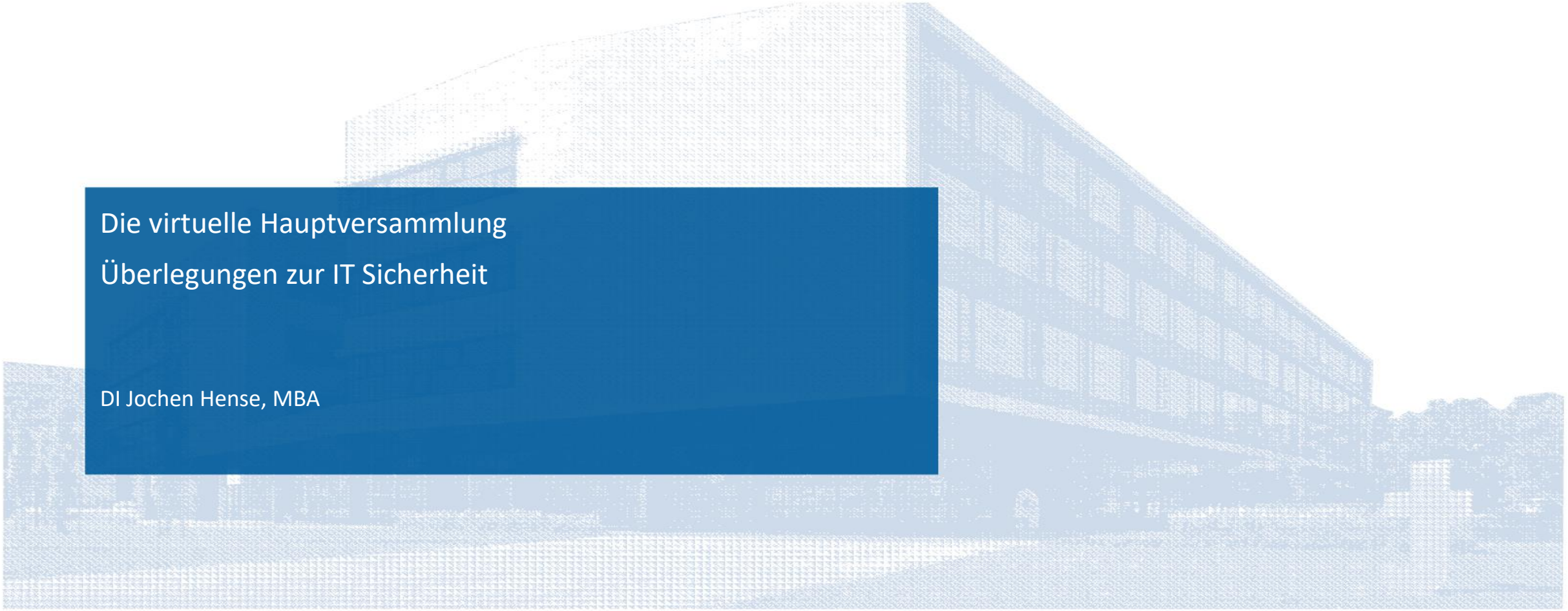


Die virtuelle Hauptversammlung

Überlegungen zur IT Sicherheit

DI Jochen Hense, MBA

- **Confidentiality**

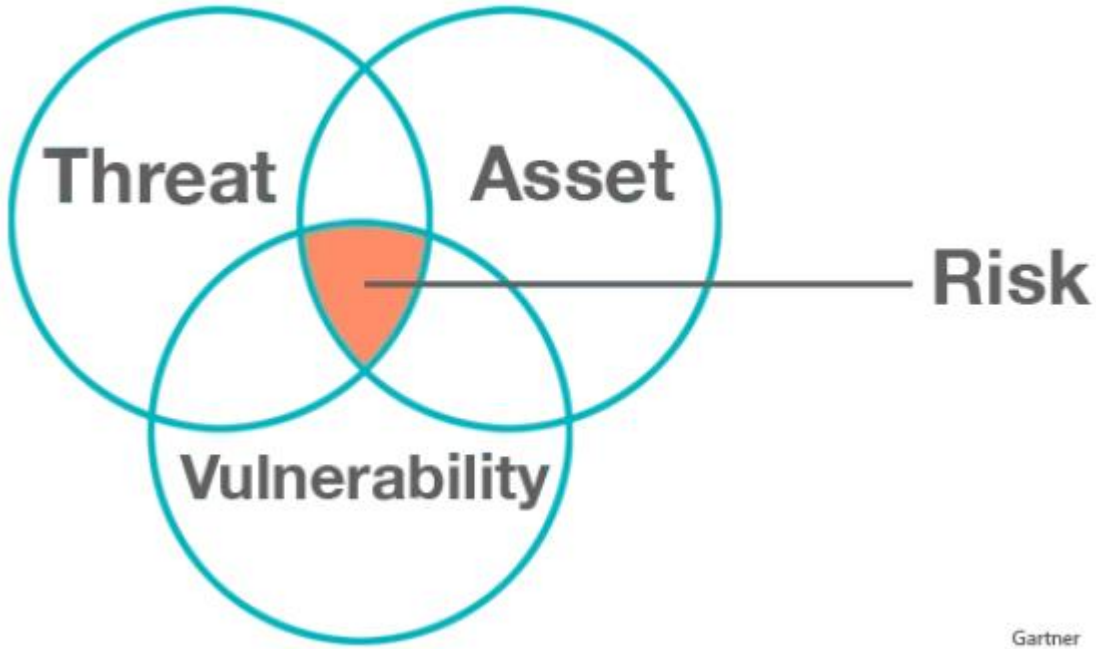
  Ensure private or confidential information is not being disclosed to unauthorized individuals.

- **Integrity**

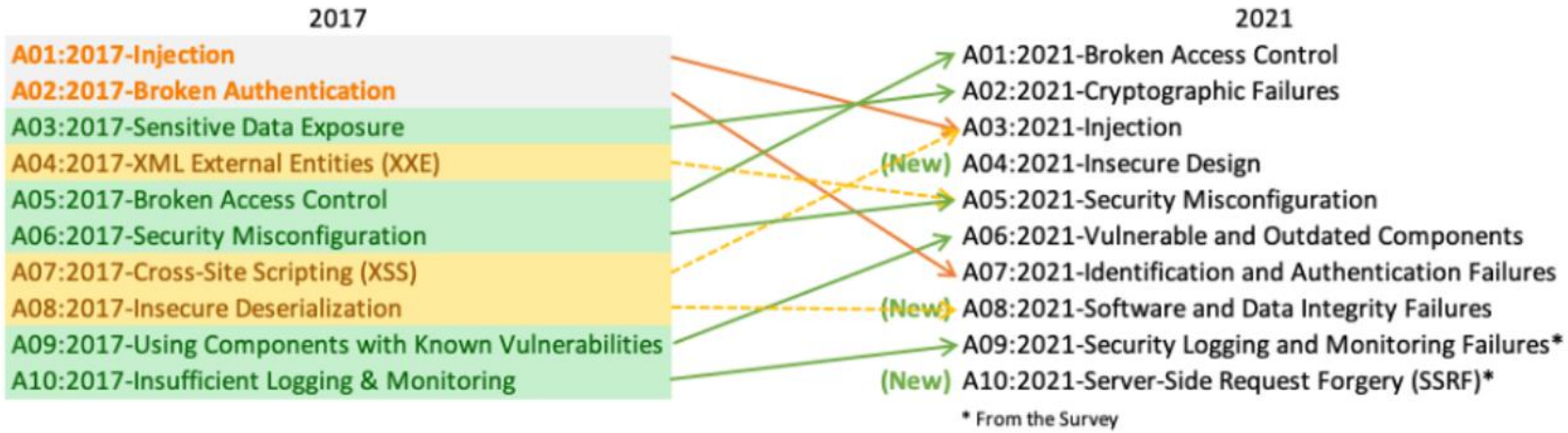
  Ensure data & systems are free from unauthorized manipulation.

- **Availability**

  Ensure systems work promptly for their intended use and service is not denied to authorized users.


Threat
Asset
Risk
Vulnerability
Gartner

OWASP Open Web Application Security Project



The OWASP® Foundation works to improve the security of software through its community-led open source software projects, hundreds of chapters worldwide, tens of thousands of members, and by hosting local and global conferences.

https://owasp.org/www-project-top-ten/

To perform virtual shareholder meetings, a tool portal typically provides the following basic use cases:

- Video and audio transmission of the meeting
- Voting by electronic absentee ballot incl. amendment/revocation
- Authorization of and instructions to the proxies of the Company
- Granting of power of attorney to a third party
- Submission of questions to the Company (in advance of the AGM)
- Declaration of objections to Annual General Meeting resolutions
- Inspection of documents (e.g. the list of attendees)
- Login/Logout

Availability

- Failure or malfunction of power supply
- Failure or technical malfunction of the online connection including mobile communications access, e.g. in areas with poor network coverage, in the event of failure of radio masts or due to overloads
- Failure or disruption of service providers
- Technical malfunctions of terminal equipment
- **Damage, loss or simple failure to carry the credential used for authentication or the mobile terminal device**
- **DoS/DDoS against video conferencing system**

Authenticity / Integrity

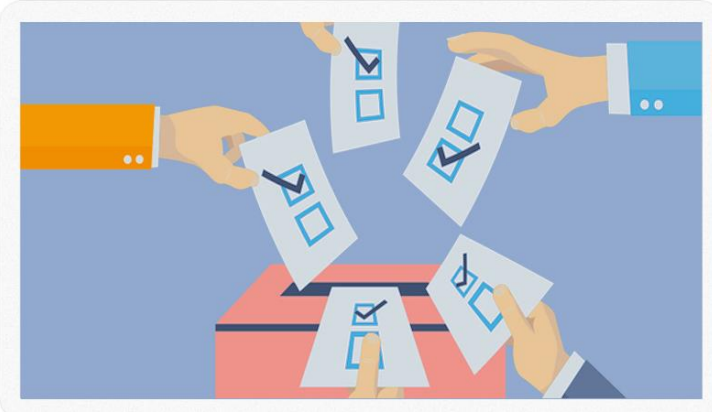
- Technical malfunctions on the end devices
- Operating errors of the user
- **Social engineering, e.g. phishing of access data to video conferences or to administrator rights**
- **Untargeted manipulation of the end device, e.g. malware infestation. When using participants' own devices (BYOD, bring-your-own-device), neither network-level security measures nor effective/homogeneous security mechanisms of BYOD devices can be relied upon**

Confidentiality

- **Listening to/viewing of the meeting/assembly by unauthorized participants.**
- **Inspection of internal meeting documents by unauthorized persons**

Availability

- Technical malfunction of the app/voting website/election software.
- **Delay or significant interference with the transmission of the vote to servers**
- **DoS/DDoS against server providing the vote as a web page or for the app, with the Consequence (e.g.)**
  - **Non-counting of an intended vote,**
  - **but also possibility of a participant to claim that own vote(s) has/have not been counted.**
- **DoS/DDoS against website that publishes voting results**

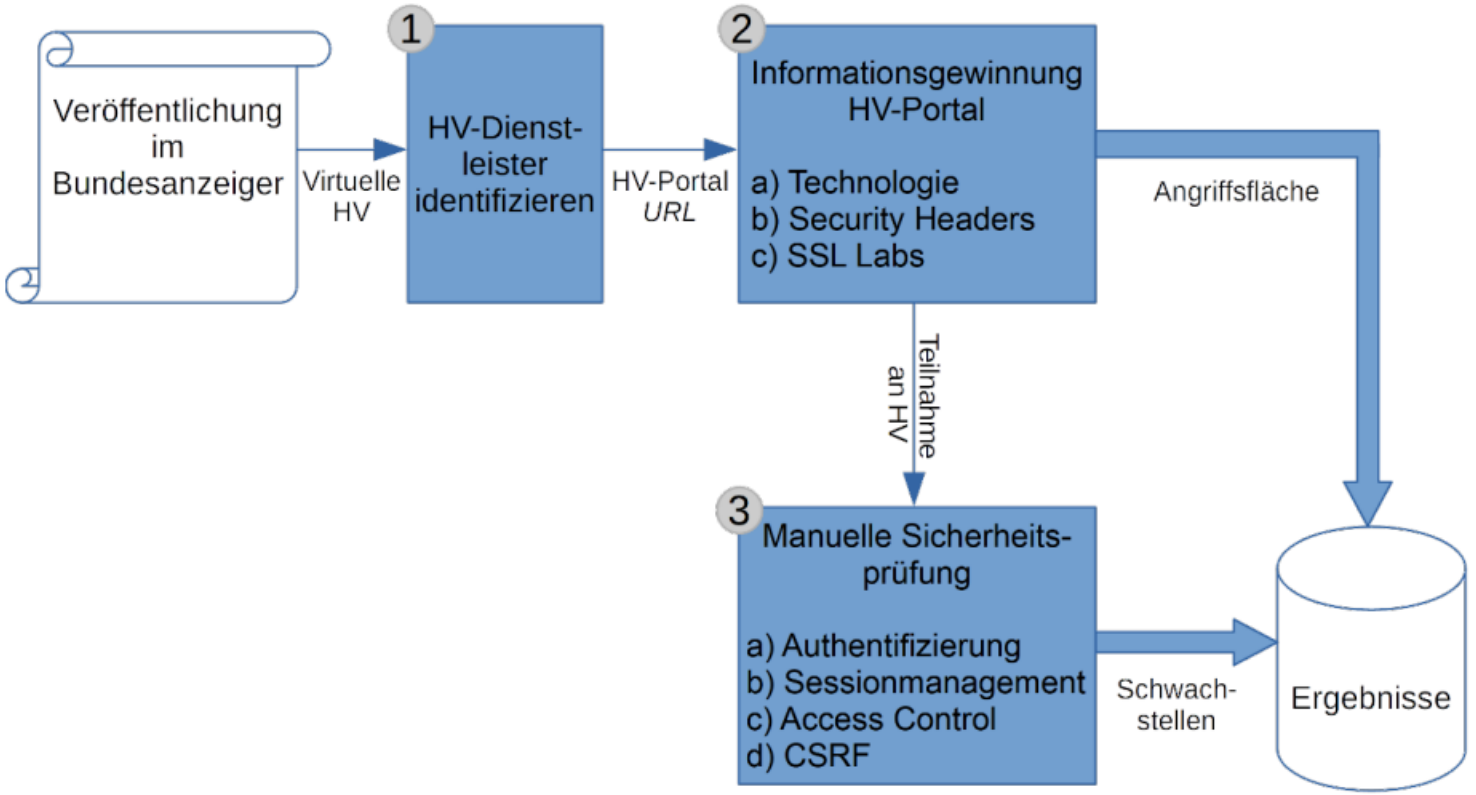


Authenticity / integrity

- **Multiple voting**
- Voting by third parties at the participant's location
- **Manipulation of the vote evaluation, e.g. by injected malicious software on Voting server**
- **Manipulation of the voting process, e.g. by attacking mobile devices with malware etc.**
- **Phishing with regard to access data for votes**
- **Manipulation of the published voting results, e.g., by injecting malware on website that publishes voting results**

Field Study Germany 2021

https://www.vipsight.eu/images/Studie_Virtuelle_Hauptversammlungen.pdf


Veröffentlichung im Bundesanzeiger
Virtuelle HV
1
HV-Dienst-leister identifizieren
HV-Portal URL
2
Informationsgewinnung HV-Portal
a) Technologie
b) Security Headers
c) SSL Labs
Angriffsfläche
Teilnahme an HV
3
Manuelle Sicherheits-prüfung
a) Authentifizierung
b) Sessionmanagement
c) Access Control
d) CSRF
Schwach-stellen
Ergebnisse

[MAYER 2021]

Kompromittiertes Schutzziel	Bedrohung	OWASP Schwachstellen-Klasse	Mögliche Angriffe
Vertraulichkeit	Angreifer kann die persönlichen Daten und/ oder das Abstimmungsverhalten von Aktionären einsehen	A2:2017 Broken Authentication A5:2017 Broken Access Control	Identitätsdiebstahl durch Brute Force- oder Session Fixation-Angriff, fehlerhafte Zugriffskontrolle
Integrität	Angreifer kann die persönlichen Daten und/ oder das Abstimmungsverhalten von Aktionären ändern	A2:2017 Broken Authentication A5:2017 Broken Access Control A8:2013 Cross-Site Request Forgery	Identitätsdiebstahl durch Brute Force- oder Session Fixation-Angriff, fehlerhafte Zugriffskontrolle, Manipulation von Daten durch CSRF-Angriff
Verfügbarkeit	Angreifer kann Accounts von Aktionären (gezielt) sperren und so die Teilnahme an der HV verhindern	A2:2017 Broken Authentication	Accounts durch Brute Force-Angriff sperren

[MAYER 2021]

oVP	Market share	C	I	A
Computershare GmbH & Co. KG	25.9%	✗		✗
Link Market Services GmbH	21.4%			
Better Orange IR & HV AG	19.5%	✗	✗	
BS portal	19.2%	✗	✗	
C-HV AG	3.1%	✗	✗	✗
ADEUS GmbH	2.9%			✗
HVBest Event-Service GmbH	1.0%	n/a	n/a	n/a
FAE Management GmbH	1.0%		✗	
∑ Broken security goals (market share)		4/8 (67.7%)	4/8 (42.8%)	3/8 (31.9%)

"In six out of eight oVPs with a market share of almost **72%**, we discovered **severe vulnerabilities**. It is important to stress, that we only investigated the oVPs against **well-known web attacks and analyzed the deployment of security best practices** in order to measure the potential attack surface. Therefore, we **only scratched on the surface** of the portals' security. Our findings are a first step to increase the security level at vAGMs and helped to sensitize the AGM service providers. "

[MAYER 2021]

Protective measures

When selecting an IT product for videoconferencing, the following factors should be considered from an information security perspective.

- **Appropriate authentication mechanisms (multi-factor authentication, if applicable)**
- Possibilities for group management and access control
- **Implementation of suitable encryption, if necessary end-to-end encryption**
- **Possibility to run the solution on an own server ("on premise"). If an own server is use, it should be hardened, e.g. by switching off or removing unneeded functionalities, Interfaces and software are switched off or removed.**
- **Auditing by independent bodies**
- **Compliance with data protection requirements**

Availability

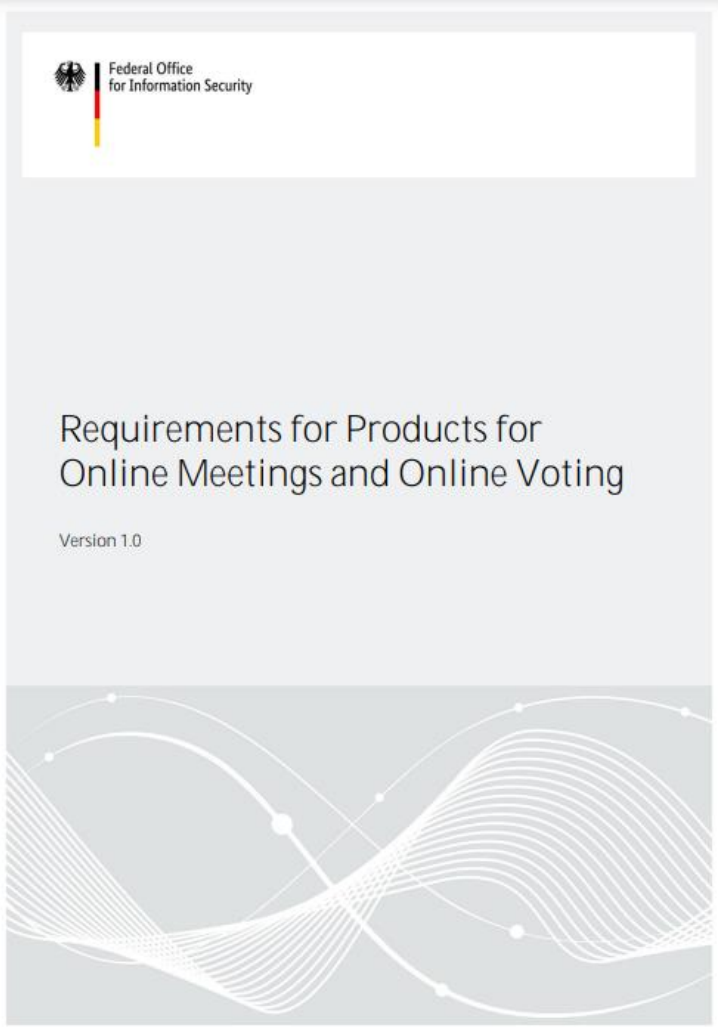
- Redundant IT equipment of the meeting management (hot standby)
- Additional dial-in option via telephone for participants
- Redundant connection of the session line to the central servers
- Emergency power supply for the central components of the session line
- Available support for operating the IT system
- Available personnel for IT support
- **Standard measures against DDoS attacks on infrastructure**

Authenticity

- **Require all participants to dial into the videoconference only with devices that have a current patch version**
- Access to the videoconference must be protected, at least by means of an access number and a sufficiently secure password, which are only made available to authorized participants
- Ensure that even when dialing in by phone, a connection to the conference is only possible with access number and password
- **Logging the session chairperson into the system via multi-factor authentication in order to obtain technical administration rights**
- **Important speakers should log on to the system via multi-factor authentication**

Integrity

- Secure connection between mobile terminal, at least of the important speakers, and central server via a Virtual Private Network (VPN) with appropriate authentication of the device registered with the central server



https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Cyber-Sicherheit/Themen/Virtuelle_Versammlungen_Abstimmungen.pdf?__blob=publicationFile&v=3