Zurück zum Inhaltsverzeichnis

Virtuelle Hauptversammlungen: Ein sicherer Ersatz für Präsenzveranstaltungen?

Prof. Dr.-Ing. Andreas Mayer[1]

Kurzfassung:
Die virtuelle Hauptversammlung (HV) ist seit März 2020 rechtlich der Präsenz-HV gleichgestellt. Sie hat sich als gesellschaftsrechtliches Kriseninstrument, während der COVID-19-Pandemie, schnell und in voller Breite etabliert. In diesem Beitrag wurden 623 virtuelle HVs empirisch erfasst und die Sicherheit der zugrundeliegenden HV-Portale systematisch auf bekannte Schwachstellen und den Einsatz von bewährten Security Best Practices hin untersucht. Bei knapp 72 % der virtuellen HVs wurden kritische Schwachstellen gefunden, welche potenziell von Angreifern ohne Spezialkenntnisse und mit geringen Ressourcen ausgenützt werden konnten. Betroffen waren u. a. virtuelle HVs großer deutscher Aktiengesellschaften aus bekannten Börsensegmenten, wie z. B. DAX und MDAX.
Nach eigenen Recherchen ist dies die erste Veröffentlichung, welche das Sicherheitsniveau von virtuellen HVs systematisch und breit angelegt untersucht. Im Ergebnis konnten die Schwachstellen behoben und so die Sicherheit von virtuellen HVs maßgeblich verbessert werden.

Stichworte: Aktionärsportal, Bedrohungsanalyse, Hauptversammlung, HV-Portal, Schutzziele, Virtuelle Versammlungen

1. Einleitung

Am 28. April 2020 veranstaltete die Bayer AG mit über 5.000 teilnehmenden Aktionären für rund 1 Million Euro die erste rein virtuelle Hauptversammlung (HV) in Deutschland[2]. Die Grundlage für die Durchführung von virtuellen HVs ist das am 27. März 2020 vom Bundesrat im Eilverfahren verabschiedete Gesetz zur Abmilderung der Folgen der COVID-19-Pandemie im Zivil-, Insolvenz- und Strafverfahrensrecht [1]. Bisher war im Aktienrecht verankert, dass die jährlich verpflichtende HV von Aktiengesellschaften zwingend als physische Präsenzveranstaltung stattfinden muss. Die Ausnahmeregelung war zunächst bis zum 31. Dezember 2020 befristet, wurde aber unlängst bis Ende 2021 verlängert [2]. Obwohl die virtuelle HV laut dem verabschiedeten Gesetz ausdrücklich nicht verpflichtend ist, hat sich mit 78 % die überwiegende Mehrheit der deutschen Aktiengesellschaften in der HV-Saison 2020 für eine präsenzlose Durchführung entschieden.

Die HV als Organ einer Aktiengesellschaft (AG) dient zur Information aller Aktionäre inkl. Frage- und Auskunftsrecht und zum Beschluss über grundsätzliche Entscheidungen, wie z. B. Entlastung von Vorstand und Aufsichtsrat, Gewinnverwendung, Wahl des Abschlussprüfers, Genehmigung dringend notwendiger Kapitalmaßnahmen oder die Abstimmung über den zwangsweisen Ausschluss der Aktionäre in einem Squeeze-Out-Verfahren. In einer virtuellen HV werden somit kritische Unternehmensentscheidungen mit teils weitreichenden Folgen getroffen und zugleich sehr sensible personenbezogene

[1] Hochschule Heilbronn, E-Mail: andreas.mayer@hs-heilbronn.de

[2] https://www.juve.de/nachrichten/deals/2020/04/aktionaerstreffen-linklaters-mandantin-bayer-spart-mit-online-hv-25-millionen-euro

Daten von Aktionären verarbeitet. Für die Durchführung von virtuellen HVs bedienen sich die Aktiengesellschaften deshalb in aller Regel eines spezialisierten HV-Dienstleisters, welcher neben organisatorischer und rechtlicher Unterstützung auch ein HV-Portal zur praktischen Durchführung der virtuellen HV im Internet zur Verfügung stellt.

In diesem Artikel werden zwei Forschungsfragen adressiert:

1. Welche HV-Dienstleister zur Abwicklung von virtuellen HVs gibt es und wie ist deren Marktanteil?
2. Wie ist das Sicherheitsniveau der HV-Portale dieser HV-Dienstleister?

Zur Beantwortung dieser beiden Forschungsfragen liefert dieser Artikel den folgenden Beitrag:

In einer Bedrohungsanalyse werden zunächst exemplarisch kritische Bedrohungen im Kontext von virtuellen HVs erarbeitet und daraus abgeleitet Schwachstellen und denkbare Angriffe auf HV-Portale vorgestellt (Kapitel 2).

Auf Grundlage der Bedrohungsanalyse wird eine Methodik zur systematischen Untersuchung der Sicherheit von HV-Portalen und deren Angriffsfläche skizziert (Kapitel 3). Dabei werden Informationen über die verwendeten Technologien gewonnen, eingesetzte Security Best Practices analysiert und die HV-Portale im Rahmen von Blackbox-Penetrationstests auf typische und weit verbreitete Schwachstellen aus der OWASP Top 10-Liste [3] untersucht[3].

In einer empirischen Studie wurden 623 virtuelle HVs von deutschen Aktiengesellschaften im Zeitraum vom 28. April 2020 – 31. Dezember 2020 analysiert. Hierbei konnten insgesamt 15 HV-Dienstleister mit acht unterschiedlichen HV-Portalen identifiziert werden. Während der systematischen Sicherheitsanalyse nahm der Autor an 46 virtuellen HVs mit 71 unterschiedlichen Accounts teil.

Im Ergebnis wiesen 71,6 % der untersuchten virtuellen HVs kritische Schwachstellen auf, welche u. a. das unbemerkte Ändern der Stimmabgabe von Aktionären, die vollständige Übernahme des Aktionärs-Accounts durch den Angreifer, das gezielte Verhindern der Durchführung von virtuellen HVs oder das Auslesen der personenbezogenen Daten von Aktionären ermöglichten. Letztere Sicherheitslücke erlaubte es, mit dem Einsatz von ca. 20 €, die personenbezogenen Daten (Name, Adresse, Geburtsdatum, …) *aller* Aktionäre, inkl. Abstimmungsverhalten und deren Anteilsbesitz, von *allen* durch den Dienstleister durchgeführten HVs auszulesen (mehr als 100 virtuelle HVs waren hiervon betroffen). Von den gefundenen Sicherheitslücken waren u. a. auch virtuelle HVs von großen DAX- und MDAX-Konzernen betroffen. Insgesamt konnten in sechs von acht HV-Portalen konkrete Schwachstellen gefunden werden. Zusammen mit den Ergebnissen der empirischen Studie und der erfassten potenziellen Angriffsfläche, werden diese Schwachstellen in Kapitel 4 dargestellt und anschließend diskutiert (Kapitel 5).

[3] Es wurden nur passive Analysen und nicht-invasive Tests mit legitimen HV-Accounts durchgeführt. Zu keinem Zeitpunkt wurden unberechtigt Daten Dritter eingesehen, verändert oder die Funktionalität der HV-Portale beeinträchtigt.

Im Rahmen von Responsible Disclosure-Verfahren, wurden die gefundenen Schwachstellen den betroffenen HV-Dienstleistern offengelegt, von diesen bestätigt und mit Unterstützung des Autors behoben.

In Kapitel 6 wird der Stand der Forschung dargestellt. Nach den Recherchen des Autors, ist dies der erste Beitrag, welcher das Sicherheitsniveau von virtuellen HVs systematisch und breit angelegt untersucht und maßgeblich verbessert hat.

2. Bedrohungsanalyse und Angreifermodell

Virtuelle HVs werden in einem HV-Portal abgehalten, welches als Webanwendung über das Internet zur Verfügung gestellt wird. Im Folgenden werden ausgehend von den Vermögenswerten (Assets), den bereitgestellten Funktionalitäten (Use-Cases) und den drei grundlegenden Schutzzielen der Informationssicherheit (Vertraulichkeit, Integrität und Verfügbarkeit) kritische Bedrohungen für HV-Portale beispielhaft dargestellt. Diese Bedrohungen können durch Schwachstellen entstehen, welche in der Anwendung bzw. der zugehörigen Infrastruktur vorhanden sind. Basierend auf den Bedrohungen und den Schwachstellen werden anschließend bekannte Angriffe skizziert, welche die Schutzziele kompromittieren können.

2.1. Assets und Funktionalitäten

In einem HV-Portal werden als wesentliche Assets die personenbezogenen Daten der für eine HV angemeldeten Aktionäre gespeichert. Diese umfassen zumindest Vorname, Name, Wohnort, Anzahl der zum Nachweisstichtag gehaltenen Aktien, Aktionärsnummer, Aktiengattung und Besitzart der Aktien (Eigen-/Fremdbesitz). Diese Daten werden auch bei einer physischen HV für das Teilnehmerverzeichnis benötigt. Regelmäßig werden jedoch weitere sensible Daten, wie z. B. vollständige Anschrift, E-Mail-Adresse, Telefonnummer, Geburtsdatum, Nationalität und die Bank, welche den Aktienbestand gemeldet hat, abgespeichert. In HV-Portalen wird zudem das Abstimmungsverhalten der einzelnen Aktionäre festgehalten.

Zur Durchführung von virtuellen HVs stellt ein HV-Portal typischerweise die folgenden grundlegenden Use-Cases bereit:

- Bild- und Tonübertragung der HV
- Stimmabgabe per elektronischer Briefwahl inkl. Änderung/Widerruf
- Vollmacht und Weisung an die Stimmrechtsvertreter der Gesellschaft
- Vollmachterteilung an einen Dritten
- Einreichung von Fragen an die Gesellschaft (im Vorfeld der HV)
- Erklärung von Widersprüchen zu Hauptversammlungsbeschlüssen
- Einsicht von Dokumenten (z. B. in das Teilnehmerverzeichnis)
- Login-/Logout

2.2. Bedrohungen, Schwachstellen und Angreifermodell

Basierend auf den vorhandenen Assets und den Use-Cases entstehen reale Bedrohungen für HV-Portale. Damit eine Bedrohung existiert, müssen eine oder mehrere Schwachstellen in der Software und/oder Infrastruktur der HV-Portale vorhanden sein, die in

einem Angriff ausgenützt werden können. Für die nachfolgend dargestellten Angriffe, besitzt der Angreifer die folgenden, leicht zu erfüllenden, Fähigkeiten:

1. Zugriff auf das HV-Portal: Die Internetadresse zum betreffenden HV-Portal wird in der HV-Einladung bzw. auf der Webseite der Gesellschaft veröffentlicht und ist für jeden einsehbar.
2. Account zum Login in das HV-Portal: Der Angreifer kann jederzeit eigene Zugangsdaten für ein von einer AG genutztes HV-Portal erhalten. Voraussetzung ist, dass er Aktien der Gesellschaft erwirbt und den Anteilsbesitz fristgerecht nachweist. Hierfür reicht es aus, dass der Angreifer eine einzige Aktie besitzt.
3. Opfer klickt auf einen Link: Weiterhin kann der Angreifer einen legitimen HV-Teilnehmer (das Opfer) dazu bringen, auf einen Link zu klicken (z. B. durch einen Beitrag in einem Diskussionsforum oder durch eine E-Mail). Das Opfer muss gleichzeitig im HV-Portal eingeloggt sein.

In Tabelle 1 werden als Ergebnis der durchgeführten Bedrohungsanalyse drei real existierende Bedrohungen aufgeführt, welche jeweils eines der drei grundlegenden Schutzziele kompromittiert. Zu jeder aufgeführten Bedrohung werden korrespondierende Schwachstellen-Klassen genannt, welche der OWASP Top 10-Liste[4] entnommen wurden. Im Speziellen werden die Schwachstellen-Klassen „A2:2017 Broken Authentication“, „A5:2017 Broken Access Control“ und „A8:2013 Cross-Site Request Forgery“ verwendet. Diese werden als Grundlage für die manuelle Blackbox-Sicherheitsprüfung der HV-Portale verwendet.

In der letzten Spalte von Tabelle 1 werden beispielhaft korrespondierende und allgemein bekannte Angriffe aufgeführt. Im Folgenden werden diese kurz erläutert:

- Identitätsdiebstahl durch einen Brute Force-Angriff: Zur Nutzung eines HV-Portals muss sich der Teilnehmer authentifizieren. Bei allen untersuchten HV-Portalen geschieht dies durch Eingabe von Benutzername und Passwort. Werden hierbei schwache Passwörter verwendet, können diese durch einen automatisierten Brute Force-Angriff erraten werden.
- Identitätsdiebstahl durch einen Session Fixiation-Angriff [4]: Bei einem Session Fixiation-Angriff benutzt das Opfer eine vom Angreifer vorgegebene Session ID. Dadurch ist die Session ID auch dem Angreifer bekannt und er kann infolgedessen die Identität des Opfers im HV-Portal übernehmen.
- Fehlerhafte Zugriffskontrolle (Broken Access Control): Authentifizierte Benutzer können in einem HV-Portal evtl. auf sensible Daten (z. B. die persönlichen Daten anderer Aktionäre) oder Funktionen zugreifen, für die sie nicht berechtigt sind. Dies ist möglich, wenn die Zugriffskontrolle fehlerhaft implementiert ist und die Berechtigungen nicht oder nur unzureichend geprüft werden.

[4] Die Open Web Application Security Project (OWASP) Foundation veröffentlicht seit 2004 regelmäßig eine anerkannte Top 10-Liste der kritischsten und häufigsten Sicherheitsprobleme von Webanwendungen.

- Cross-Site Request Forgery (CSRF) [5]: Bei einem CSRF-Angriff führt das Opfer, meist unbewusst, vom Angreifer vorgegebene Aktionen aus. Dies kann bei einem HV-Portal z. B. das Ändern des Abstimmungsverhaltens sein.
- Sperren von Accounts durch einen Brute Force-Angriff: Eine häufig eingesetzte Gegenmaßnahme, um das automatisierte Erraten von Passwörtern zu verhindern, ist das Sperren von Benutzeraccounts nach mehrmaliger Falscheingabe. Jedoch kann dadurch auch ein legitimer HV-Teilnehmer nicht mehr an der HV teilnehmen. Wenn der Angreifer den Aufbau und die Vergaberichtlinien der Benutzeraccounts kennt, kann er gezielt einzelne oder alle Teilnehmer von einer HV ausschließen.

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 Fixiation-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 Fixiation-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

Tabelle 1: Die Ergebnisse der Bedrohungsanalyse

3. Methodik

Nachfolgend wird die für die systematische Sicherheitsanalyse verwendete Methodik, welche in Abbildung 1 dargestellt wird, beschrieben.

Als Datenquelle wurden die von der Bundesanzeiger Verlag GmbH[5] veröffentlichten Einberufungen von HVs herangezogen. Anhand dieser Bekanntmachungen wurde geprüft, ob es sich um eine virtuelle HV handelt und wann diese stattfindet. Im Falle einer virtuellen HV wurden die folgenden Analyseschritte durchgeführt:

[5] https://www.bundesanzeiger.de/

1. HV-Dienstleister identifizieren: Mithilfe der im Bundesanzeiger bekanntgemachten HV-Einladung und den auf der Webseite der AG veröffentlichten Informationen wurde der HV-Dienstleister identifiziert und der Link (*HV-Portal URL*) zu dem HV-Portal extrahiert.
2. Informationsgewinnung: Um die potenzielle Angriffsfläche abzuschätzen und einen Eindruck über die verwendeten Security Best Practices zu gewinnen, wurde das HV-Portal in einem ersten Schritt untersucht. Hierbei wurden die folgenden öffentlich verfügbaren Informationen gewonnen:

    a) Verwendete Technologien: Die freie Browser Extension Wappalyzer [6] und die manuelle Untersuchung der HTTP-Header, lieferten die Datenbasis für die eingesetzten Softwarebibliotheken und die verwendeten Infrastrukturkomponenten. Weiterhin wurde untersucht, ob veraltete Softwarebibliotheken mit bekannten Schwachstellen eingesetzt werden.

    b) Eingesetzte Security Header: Es existieren heutzutage eine Vielzahl von anerkannten und bewährten HTTP Security Header (z. B. HSTS[6]), welche benutzt werden können, um die Sicherheit von Webanwendungen zu erhöhen. Der Einsatz dieser Security Header wurde mit dem kostenfreien Dienst Security Headers [7] untersucht. Als Ergebnis wird ein Rating von A+ (sehr gut) bis F (ungenügend) vergeben.

    c) Benutzte TLS-Konfiguration: Ein weiterer wichtiger Baustein für die Sicherheit des HV-Portals ist der Einsatz des TLS-Protokolls, um die Datenübertragung per HTTPS hinsichtlich Vertraulichkeit, Integrität und Authentizität abzusichern. Der kostenfreie Dienst SSL Labs [8] wurde eingesetzt, um die Sicherheit der übertragenen Daten zu beurteilen. Als Ergebnis wird ein Rating von A+ (sehr gut) bis F (ungenügend) vergeben.

3. Manuelle Sicherheitsprüfung: Sofern es möglich war, wurden Aktien der Gesellschaft erworben und HV-Eintrittskarten angefordert, um das HV-Portal tiefgreifender auf Schwachstellen zu untersuchen. Aufbauend auf den Ergebnissen aus der Bedrohungsanalyse, wurden dabei die folgenden sicherheitsrelevanten Bereiche untersucht:
    a) Authentifizierung
    b) Sessionmanagement
    c) Zugriffskontrolle (Access Control)
    d) CSRF

Die Ergebnisse aus Schritt 2 (potenzielle Angriffsfläche) und Schritt 3 (evtl. vorhandene Sicherheitslücken), flossen anschließend in die empirische Studie über das Sicherheitsniveau von virtuellen HVs ein (siehe Kapitel 4).

---

[6] HTTP Strict Transport Security (HSTS) ist ein Sicherheitsmechanismus für HTTPS-Verbindungen, der u. a. vor Downgrade-Angriffen und Session Hijacking schützen soll.

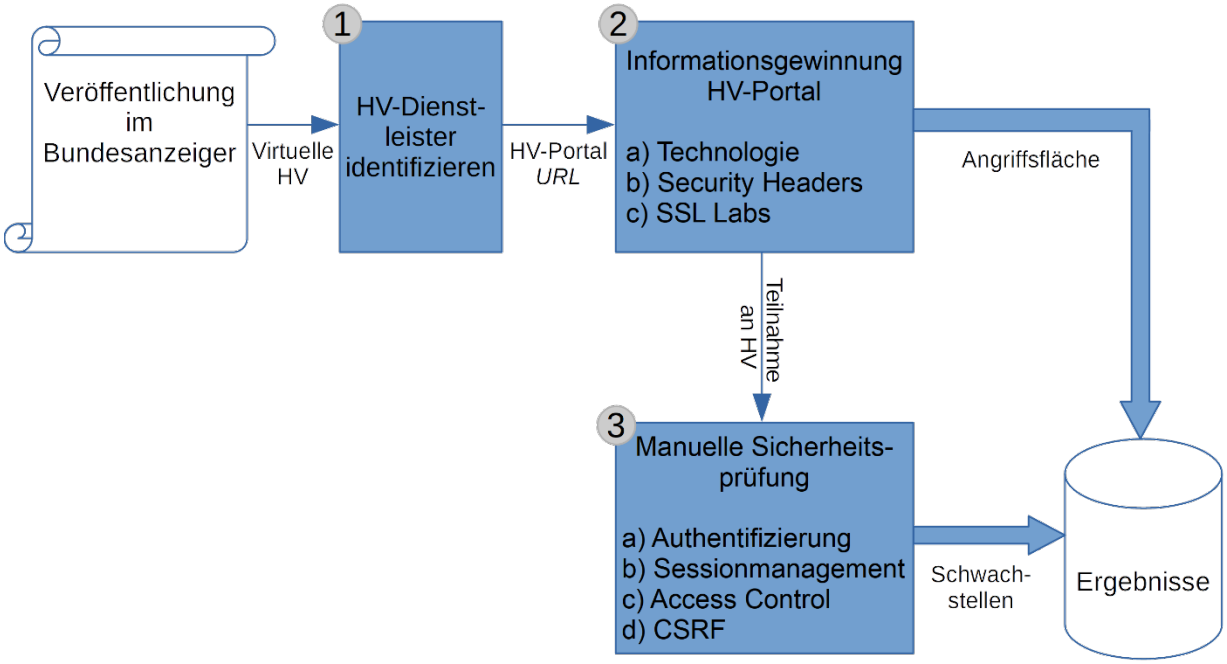

Abbildung 1: Die Methodik der Sicherheitsuntersuchung von virtuellen HVs

4. Ergebnisse

Für diese Studie wurden die virtuellen HVs der HV-Saison 2020 empirisch erfasst und nach der in Kapitel 3 vorgestellten Methodik systematisch untersucht. Hierfür nahm der Autor an 46 virtuellen HVs mit 71 unterschiedlichen Accounts teil. Der Auswertungszeitraum beginnt mit der ersten virtuellen HV (Bayer AG) am 28.04.2020 und endet am 31.12.2020. Insgesamt wurden in diesem Zeitraum 623 virtuelle HVs durchgeführt, wovon bei zwei HVs der HV-Dienstleister nicht identifiziert werden konnte. Von den verbleibenden 621 virtuellen HVs wurden 584 (94 %) von 15 unterschiedlichen HV-Dienstleistern durchgeführt. In 23 Fällen (3,7 %) wurde ein Videokonferenzsystem, wie z. B. Zoom, ohne ein spezielles HV-Portal eingesetzt. Hierbei fand die Abstimmung über die Tagesordnung typischerweise konventionell per Brief, Fax oder E-Mail statt. Bei 14 virtuellen HVs (2,3%) wurden eigene Softwarelösungen eingesetzt, welche für diesen Zweck von den AGs selbst oder durch Dritte entwickelt wurden. Die Verteilung der virtuellen HVs auf die einzelnen HV-Dienstleister kann Abbildung 2 entnommen werden. Die per Videokonferenzsystem durchgeführten HVs und die eigenentwickelten HV-Portallösungen werden im Folgenden nicht weiter betrachtet.

Bei der weiterführenden Untersuchung der einzelnen HV-Portale stellte es sich heraus, dass die HV-Dienstleister UBJ. GmbH, GFEI AG, ITTEB GmbH & Co. KG, BADER & HUBL GmbH, HV-Management GmbH, AAA HV Management GmbH, Art of Conference und HV AG alle dieselbe technische HV-Plattform, im Folgenden „BS HV-Portal“ genannt, einsetzen. Aufgrund dieser Tatsache reduziert sich die Anzahl der unterschiedlichen von HV-Dienstleistern eingesetzten HV-Portale auf acht Plattformen.

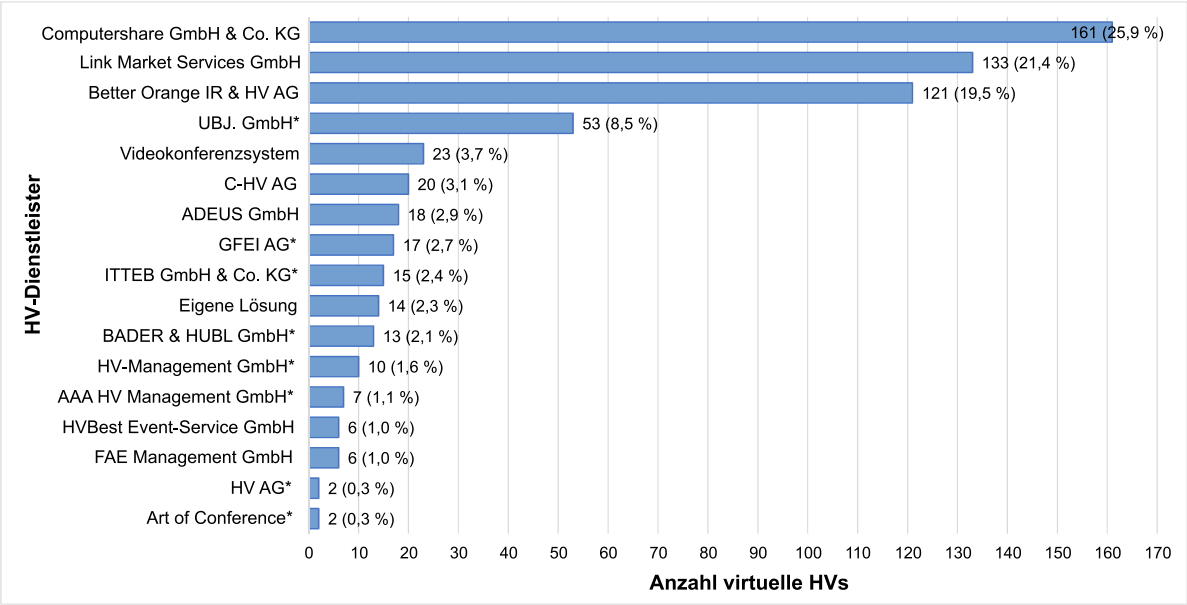

Abbildung 2: Anzahl der virtuellen HVs pro HV-Dienstleister inkl. Prozentangaben (*: HV-Dienstleister, welche dieselbe technische Plattform benutzen)

Die HV-Portale der drei größten HV-Dienstleister Computershare GmbH & Co. KG, Link Market Services GmbH und Better Orange IR & HV AG dominieren den Markt für virtuelle HVs mit insgesamt 66,8 % Marktanteil. Hinzu kommt das BS HV-Portal, welches von acht HV-Dienstleistern benutzt wird und in Summe auf gerundet 19,2 % Marktanteil kommt. Die restlichen 8 % teilen sich die HV-Portale der vier HV-Dienstleister C-HV AG (3,1 %), ADEUS Aktienregister-HV-Service GmbH (2,9 %), HVBest Event-Service GmbH (1,0 %) und die FAE Management GmbH (1,0 %) auf.

4.1. Informationsgewinnung

Bei den untersuchten HV-Portalen handelt es sich in sieben von acht Fällen um klassische Webanwendungen mit serverseitiger Anwendungslogik. Lediglich die Computershare GmbH & Co. KG setzt auf eine moderne Javascript-basierte Single Page Anwendung. Zur Realisierung werden die unterschiedlichsten Programmiersprachen (1x Javascript, 2x PHP, 2x ASP.NET und 3x Java), Frameworks (Angular JS, JavaServer Pages, Java Server Faces, Telerik Web UI und CodeIgniter) und Webserver (3x Microsoft IIS, 2x Nginx und 1x Apache) eingesetzt. In zwei Fällen konnte der Webserver der HV-Portalsoftware nicht identifiziert werden.

In fünf von acht HV-Portalen wurden insgesamt zehn veraltete Softwarebibliotheken mit bekannten Schwachstellen gefunden (Marktanteil: 52,4 %). Die verwundbaren Bibliotheken stammen aus den Jahren 2015-2019. Bei den Anbietern Link Market Services GmbH, BS HV-Portal und HVBest Event-Service GmbH wurden keine veralteten Softwarekomponenten mit bekannten Schwachstellen entdeckt.

Alle HV-Portale sind per HTTPS erreichbar und setzen das TLS-Protokoll ein. Vier von acht HV-Portale erreichten lediglich ein B-Rating (Marktanteil: 49,2 %). Die drei Anbieter Link Market Services GmbH, Better Orange IR & HV AG und FAE Management

GmbH (Marktanteil: 41,9 %) konnten ein A-Rating vorweisen. Lediglich das HV-Portal der ADEUS GmbH erreichte mit A+ das beste mögliche Rating (Marktanteil: 2,9 %).

Beim Security Header-Rating konnten die Computershare GmbH & Co. KG und die ADEUS GmbH mit einem befriedigenden C-Rating am besten abschneiden (Marktanteil: 28,8%). Die HVBest Event-Service GmbH erzielte ein D-Rating. Die restlichen HV-Portale, mit einem Marktanteil von 64,2 %, erreichten mit einem F-Rating die schlechteste mögliche Note.

In Tabelle 2 werden die beschriebenen Ergebnisse zusammenfassend dargestellt.

HV-Portal	Technologie	Verwundbare Software	SSL Labs Rating	Security Header Rating
Computershare GmbH & Co. KG	Microsoft IIS und Angular JS	Ja (Webserver und Javascript Bibliotheken)	B	C
Link Market Services GmbH	Webserver unbekannt, PHP	Nein	A	F
Better Orange IR & HV AG	Nginx und Java Server Faces	Ja (Webserver)	A	F
BS HV-Portal	Microsoft IIS, ASP.NET mit Telerik Web UI	Nein	B	F
C-HV AG	Microsoft IIS, ASP.NET mit Telerik Web UI	Ja (Javascript Bibliothek)	B	F
ADEUS GmbH	Webserver unbekannt, Java	Ja (Javascript Bibliothek)	A+	C
HVBest Event-Service GmbH	Nginx und JavaServer Pages	Nein	B	D
FAE Management GmbH	Apache, PHP und CodeIgniter	Ja (Javascript Bibliotheken, CodeIgniter)	A	F

Tabelle 2: Die Ergebnisse der Informationsgewinnung aus Schritt 2 der Methodik (Legende Rating: A=sehr gut, F=ungenügend)

4.2. Manuelle Sicherheitsprüfung

Im Rahmen der manuellen Blackbox-Sicherheitsprüfung wurde zunächst die Passwort-basierte Authentifizierung untersucht. Die Ergebnisse werden in Tabelle 3 dargestellt.

Alle HV-Dienstleister verwenden als Benutzername eine numerische Zahl, welche aufsteigend aus einem festen Nummernkreis vergeben wird (meist 4- oder 5-stellig mit führenden Nullen). Durch diese Art der Accountvergabe, sind die Benutzernamen sehr leicht zu erraten.

Basierend auf den 71 untersuchten HV-Accounts werden, je nach HV-Dienstleister, unterschiedliche Passwort-Richtlinien eingesetzt. Bis auf eine Ausnahme, vergeben alle

Dienstleister zufällig generierte Passwörter. Die Länge beträgt 5-10 Zeichen, wobei von den verfügbaren Zeichen Groß-, Kleinbuchstaben und Zahlen verwendet werden. Als Sonderzeichen kommt nur in einem Fall das „*“-Zeichen zum Einsatz. Das HV-Portal der HVBest Event-Service GmbH verwendet zur Authentifizierung kein zufälliges Passwort, sondern eine Kombination aus Anzahl der gehaltenen Aktien, PLZ und Wohnort des Aktionärs[7]. Die Passwort-Richtlinien der HV AG und der Art of Conference konnten nicht untersucht werden, da keine Zugangsdaten zur Verfügung standen (Marktanteil: 0,6 %).

Die HV-Portale von Better Orange IR & HV AG und HVBest Event-Service GmbH zeigen dem Anwender an, ob entweder Benutzername oder Passwort falsch eingegeben wurden (Marktanteil: 20,5 %). Dieses Verhalten liefert wertvolle Informationen über die Existenz von gültigen Accounts.

Die HV-Dienstleister Link Market Services GmbH und HVBest Event-Service GmbH sichern den Login zusätzlich über Captchas[8] ab, welche für einen erfolgreichen Login korrekt gelöst werden müssen (Marktanteil: 22,4 %).

Bei den HV-Portalen der Computershare GmbH & Co. KG, C-HV AG, ADEUS GmbH und FAE Management GmbH führte die mehrfache Eingabe von falschen Passwörtern zur Sperrung des jeweiligen Accounts (Marktanteil: 32,9 %). Während diese Sperrung bei der FAE Management GmbH nach ca. 30 Minuten wieder aufgehoben wird, können die Accounts bei den anderen drei Dienstleistern nur manuell durch den Support entsperrt werden. Bei allen anderen HV-Dienstleistern erfolgt durch die wiederholte Eingabe falscher Passwörter keine Sperrung von existierenden Accounts.

Im Bereich des Sessionmanagements waren die drei HV-Portale von Better Orange IR & HV AG, BS HV-Portal und C-HV AG für Session Fixiation-Angriffe anfällig (Marktanteil: 41,8 %). Bei der Better Orange IR & HV AG und der Computershare GmbH & Co. KG war die Logout-Funktionalität des HV-Portals wirkungslos (Marktanteil: 45,4 %). Als Konsequenz blieb die Benutzersession trotz Logout des Users gültig.

Die Untersuchungen im Bereich Broken Access Control offenbarten bei der Computershare GmbH & Co. KG (Marktanteil: 25,9 %) eine sehr kritische Schwachstelle, welche das Schutzziel der Vertraulichkeit betraf. Bei allen anderen HV-Dienstleistern wurden keine Schwachstellen im Bereich der Zugriffskontrolle gefunden.

Für CSRF-Angriffe war lediglich die FAE-Management GmbH anfällig. Hierdurch konnte z. B. das Abstimmungsverhalten des Opfers unbemerkt verändert werden.

Die beschriebenen Sachverhalte aus der Sicherheitsuntersuchung der Bereiche Sessionmanagement, Access Control und CSRF werden in Tabelle 4 zusammengefasst.

---

[7] Nach Rücksprache mit dem Dienstleister unterstützt dieser auch alternative Authentifizierungsverfahren und hat diese auch im Einsatz.

[8] Captchas sind kleine Aufgaben, welche in diesem Kontext dazu dienen, Brute Force-Angriffe zu erschweren. Sie sollen von Menschen (zumeist) effizient und von Maschinen nicht lösbar sein.

HV-Portal	Passwort-Richtlinie	Anzeige Passwort /Account falsch?	Captcha vorhanden?	Account sperrbar?
Computershare GmbH & Co. KG	6-stellig [A-Z, a-z, 0-9] oder [A-Z, a-z]	Nein	Nein	Ja
Link Market Services GmbH	6-stellig [0-9]	Nein	Ja	Nein
Better Orange IR & HV AG	8-stellig [A-Z, a-z, 0-9, *]	Ja	Nein	Nein
UBJ. GmbH	5-stellig [A-Z, a-z, 0-9] oder 8-stellig [0-9]	Nein	Nein	Nein
C-HV AG	8-stellig [A-Z, 0-9]	Nein	Nein	Ja
ADEUS GmbH	10-stellig [0-9]	Nein	Nein	Ja
GFEI AG	5- oder 6-stellig [A-Z, a-z, 0-9]	Nein	Nein	Nein
ITTEB GmbH & Co. KG	6-stellig [A-Z, a-z, 0-9]	Nein	Nein	Nein
BADER & HUBL GmbH	10-stellig [a-z, 0-9]	Nein	Nein	Nein
HV-Management GmbH	8-stellig [A-Z, a-z, 0-9]	Nein	Nein	Nein
AAA HV GmbH	5-stellig [0-9]	Nein	Nein	Nein
HVBest Event-Service GmbH	Anzahl Aktien, PLZ und Ort	Ja	Ja	Nein
FAE Management GmbH	8-stellig [0-9, a-f]	Nein	Nein	Ja (temporär für ca. 30 Min.)
HV AG	n/a	Nein	Nein	Nein
Art of Conference	n/a	Nein	Nein	Nein

Tabelle 3: Die Ergebnisse aus der Untersuchung der Passwort-basierten Authentifizierung

HV-Portal	Sessionmanagement		Broken Access Control	CSRF-Angriff möglich?
	Session Fixiation-Angriff möglich?	Session-Logout wirksam?		
Computershare GmbH & Co. KG	Nein	Nein	Ja	Nein
Link Market Services GmbH	Nein	Ja	Nein	Nein
Better Orange IR & HV AG	Ja	Nein	Nein	Nein
BS HV-Portal	Ja	Ja	Nein	Nein
C-HV AG	Ja	Ja	Nein	Nein
ADEUS GmbH	Nein	Ja	Nein	Nein
HVBest Event-Service GmbH	n/a	n/a	n/a	n/a
FAE Management GmbH	Nein	Ja	Nein	Ja

Tabelle 4: Die Ergebnisse der Sicherheitsuntersuchung der Bereiche Sessionmanagement, Access Control und CSRF

5. Diskussion

Nachfolgend werden die in Kapitel 4 dargestellten Ergebnisse diskutiert und bewertet.

5.1. Informationsgewinnung

Bei fünf von acht HV-Portalen, mit einem Marktanteil von 52,4 %, wurden verwundbare Softwarekomponenten verwendet. Hierbei ist anzumerken, dass durch den Einsatz von anfälligen Softwarebibliotheken nicht zwangsläufig die dort enthaltenen Schwachstellen ausgenutzt werden können. Es ist z. B. möglich, dass die verwundbare Funktionalität überhaupt nicht benutzt wird. Jedoch gehört es zu den anerkannten Security Best Practices, verwundbare Softwarekomponenten möglichst zeitnah zu patchen. Dies zeigt, dass es aus Sicherheitssicht im Patchmanagement einiger HV-Dienstleister noch Optimierungspotenzial gibt. Insbesondere, da die gefundenen Schwachstellen bereits 1-5 Jahre bekannt waren und Sicherheitsupdates existierten.

Die TLS-Konfiguration der HV-Portale offenbarte keine gravierenden Schwachstellen. Das B-Rating, welches der Hälfte der Anbieter vergeben wurde, beruht auf der serverseitigen Unterstützung der veralteten Protokollversionen TLS 1.0 und TLS 1.1. Jedoch werden beide Versionen bereits seit Mitte 2018 aus Sicherheitsgründen nicht mehr zum praktischen Einsatz empfohlen [9], [10]. Werden sie abgeschaltet, kann das Rating auf A und damit auf ein sehr gutes Sicherheitsniveau verbessert werden.

Im Bereich der Security Header wird leider sehr viel Potenzial für die Gesamtsicherheit der HV-Portale verschenkt, zumal es sich hierbei um eine Vielzahl von breit unterstützten und etablierten Security Best Practices handelt. Durch deren Einsatz können viele

bekannte Angriffe effektiv unterbunden werden. Diese aus Sicherheitssicht „Low Hanging Fruits“ können ohne großen Aufwand und innerhalb kürzester Zeit implementiert werden. Dies zeigen auch die Rückmeldungen und bereits umgesetzten Optimierungen der HV-Dienstleister.

Insgesamt zeigen die Ergebnisse aus der Informationsgewinnung, dass die potenzielle Angriffsfläche der HV-Portale noch deutlich verringert werden kann.

5.2. Manuelle Sicherheitsprüfung

Für die Aktionärs-Accounts erzeugen sieben von acht HV-Dienstleistern zufällig generierte Passwörter und verhindern somit schwache Kennwörter, wie z. B. „12345“ oder den Einsatz derselben Passwörter bei unterschiedlichen Diensten.

Nach den Empfehlungen des Bundesamtes für Sicherheit in der Informationstechnik, sollte ein sicheres Passwort, nach Stand der Technik, mindestens acht Zeichen lang sein und aus Groß- und Kleinbuchstaben, Ziffern und Sonderzeichen bestehen. Passwörter, welche nicht alle vier Zeichenarten verwenden, sollten deutlich länger sein (>12 Zeichen) oder mit einer Mehr-Faktor-Authentisierung abgesichert werden [11].

Bei den untersuchten HV-Portalen wurden diese Vorgaben von keinem Anbieter erfüllt. Die geringste Passwort-Komplexität wies die AAA Management HV GmbH auf (10^5 mögliche Passwort-Kombinationen). Die HVBest Event-Service GmbH verwendet keine Passwörter, sondern erwartet neben dem Benutzernamen die richtige Eingabe von Aktienanzahl, PLZ und Wohnort des Aktionärs. Diese Art der Authentifizierung ist als relativ schwach anzusehen, da die notwendigen Informationen leicht beschaffbar (PLZ und Wohnort eines Aktionärs) bzw. erratbar sind (Aktienanzahl).

In der Diskussion mit den HV-Dienstleistern wurde als Grund für die niedrigere Passwort-Komplexität der geringere Supportaufwand angeführt. Im Hinblick auf die Kritikalität der Zugangsdaten im Kontext von virtuellen HVs und das verfügbare Angreifer-Zeitfenster von bis zu 12 Tagen[9], sind komplexere Passwort-Richtlinien bzw. die Verwendung einer Mehrfaktor-Authentifizierung sehr zu empfehlen.

HVBest Event-Service GmbH und Link Market Services GmbH sichern den Login zusätzlich durch Captchas ab. Hierdurch soll ein Brute Force-Angriff erschwert werden. Jedoch sind die verwendeten Captchas sehr einfach aufgebaut und verwenden nur eine geringe Anzahl von möglichen Zeichen (siehe Abbildung 3). Wie in [12] gezeigt wurde, kann diese Art von Captchas automatisiert gelöst werden.

Abbildung 3: Beispiele für Captchas der Link Market Services GmbH (links) und der HVBest Event-Service GmbH (rechts)

[9] 12 Tage vor einer HV ist der Nachweisstichtag über den Anteilsbesitz ([1], Artikel 2, §1 Abs. 3). Spätestens ab diesem Zeitpunkt ist das HV-Portal aktiv zu schalten.

Um das systematische Erraten von Passwörtern zu verhindern, sperren vier HV-Dienstleister nach mehrmaliger Falscheingabe den zugehörigen Benutzeraccount. Dadurch eröffnet sich aber die Möglichkeit eines Brute Force-Angriffs auf die Verfügbarkeit des HV-Portals. Die FAE Management GmbH entschärft diese Bedrohung, indem die Accounts automatisch nach ca. 30 Minuten wieder entsperrt werden. Problematisch ist in diesem Zusammenhang, dass alle Dienstleister vorhersehbare Benutzernamen einsetzen. Dadurch ist es möglich, kurz vor einer HV, gezielt einzelne oder alle Aktionärs-Accounts zu sperren. Zudem können bei der Better Orange IR & HV AG und der HVBest Event-Service GmbH (Marktanteil: 20,5 %) gültige Accounts aufgrund der Fehlermeldung vom Angreifer identifiziert werden. Es wird daher als Security Best Practice geraten, bei fehlerhaften Loginversuchen immer generische Fehlermeldungen anzuzeigen (z. B. „Login fehlgeschlagen!“).

Die im Bereich Sessionmanagement nachgewiesenen Session Fixiation-Angriffe zeigten, dass bei drei HV-Portalen (45,8 % Marktanteil) der Angreifer die Benutzersession des Opfers vollständig übernehmen kann. Grundlegend hierfür war, dass dem HV-Teilnehmer, nach erfolgreicher Authentifizierung, keine neue Session ID vergeben wurde. Die bei zwei HV-Portalen (Marktanteil: 45,4 %) nicht wirksame Logout-Funktionalität eröffnete ebenfalls die Möglichkeit der vollständigen Übernahme der Session. Diese kann z. B. dadurch übernommen werden, dass der Angreifer nach dem ordnungsgemäßen Logout des Opfers Zugriff auf die im Browser weiterhin gespeicherten Sessiondaten bekommt.

Im Bereich fehlerhafte Zugriffskontrolle ist die im HV-Portal des größten HV-Dienstleisters (Marktanteil: 25,9 %) gefundene Schwachstelle als sehr kritisch einzustufen. Sie erlaubte es, die personenbezogenen Daten (Name, Adresse, Geburtsdatum, usw.) *aller* Aktionäre, inkl. Abstimmungsverhalten und deren Anteilsbesitz, von *allen* durchgeführten virtuellen HVs auszulesen. Hierfür war lediglich ein gültiger Account für eine beliebige HV notwendig.

Der bei einem HV-Portal (Marktanteil: 1,0 %) durchführbare CSRF-Angriff erlaubte es, durch Klick des Opfers auf einen Link das Abstimmungsverhalten zu ändern.

Tabelle 5 zeigt, basierend auf den praktisch nachgewiesenen Angriffen, die verletzten Schutzziele je HV-Portal. Dabei wurden die schwachen Passwort-Richtlinien, welche zu einem Verlust der Vertraulichkeit und Integrität führen können, nicht mit einbezogen. Hintergrund: Brute Force-Angriffe wurden bei den Untersuchungen nicht durchgeführt, um die Funktionalität der HV-Portale nicht zu gefährden. Jedoch haben alle kontaktierten HV-Dienstleister diese Angriffsmöglichkeit als sicherheitsrelevant eingestuft.

Insgesamt wurde bei sechs von acht HV-Portalen (Marktanteil: 71,6 %), mindestens ein Schutzziel auf Basis der Bedrohungsanalyse und der dort gezeigten Auswirkungen kompromittiert. Lediglich das HV-Portal der Link Market Services GmbH wies keine praktisch nachgewiesenen Angriffsmöglichkeiten auf. Das HV-Portal HVBest Event-Service GmbH konnte aufgrund fehlender Zugangsdaten nicht vollumfänglich getestet werden. Dennoch zeigt die Analyse der Angriffsfläche, dass auch bei diesen Anbietern durchaus Potenzial zur Erhöhung des Sicherheitsniveaus besteht.

HV-Portal	Marktanteil	Kompromittiertes Schutzziel		
		Vertraulichkeit	Integrität	Verfügbarkeit
Computershare GmbH & Co. KG	25,9 %	X		X
Link Market Services GmbH	21,4 %			
Better Orange IR & HV AG	19,5 %	X	X	
BS HV-Portal	19,2 %	X	X	
C-HV AG	3,1 %	X	X	X
ADEUS GmbH	2,9 %			X
HVBest Event-Service GmbH	1,0 %	n/a	n/a	n/a
FAE Management GmbH	1,0 %		X	

Tabelle 5: Darstellung der kompromittierten Schutzziele der untersuchten HV-Portale

6. Stand der Forschung

Die bisherigen Veröffentlichungen im Bereich virtuelle HVs beschränken sich weitgehend auf deren juristische, organisatorische und technische Risiken. In [13] untersucht C. Danwerth empirisch die rechtlichen Modalitäten und Gestaltungsvarianten von virtuellen HVs. Die ermittelten Marktanteile der drei größten Dienstleister für virtuelle HVs decken sich mit den Ergebnissen dieses Beitrags.

M. Scholze und M. Kaspar zeigen in [14], dass der Fokus bei virtuellen HVs auf einer rechtssicheren und störungsfreien Durchführung liegt. Aspekte der IT-Sicherheit spielen hierbei keine oder nur eine untergeordnete Rolle. Auf der anderen Seite beklagen Aktionärsvereinigungen berechtigterweise die juristisch begründeten Einschränkungen der Aktionärsrechte durch das neue virtuelle Format [15], [16].

7. Fazit und Ausblick

Virtuelle HVs haben sich innerhalb kürzester Zeit als ein systemrelevantes Kriseninstrument etabliert. Neben allen juristischen, organisatorischen und technischen Aspekten werden virtuelle HVs langfristig nur bei einem ausreichend hohen Sicherheitsniveau erfolgreich sein. Die Ergebnisse der ersten empirisch und systematisch durchgeführten Sicherheitsuntersuchung von virtuellen HVs zeichnet dabei ein verbesserungswürdiges Bild der Sicherheitslage. In sechs von acht HV-Portalen, mit einem Marktanteil von 71,6 %, wurden kritische Sicherheitslücken gefunden.

Im Hinblick auf die aktuelle und zukünftig sicher zunehmende Wichtigkeit von virtuellen HVs ist hier weiterer Handlungsbedarf zu sehen. Im Rahmen dieses Beitrags konnten die betroffenen HV-Dienstleister sensibilisiert werden. In einem ersten Schritt wurde gemeinsam mit ihnen das Sicherheitsniveau der HV-Portale deutlich erhöht. Hierbei ist positiv zu erwähnen, dass alle Beteiligten sehr professionell agierten und zeitnah die gemeldeten Schwachstellen behoben haben. Darüber hinaus wurden viele der genannten Security Best Practices (z. B. der Einsatz von Security Headern, komplexere Passwort-Richtlinien und aktives Patchmanagement) proaktiv umgesetzt.

Literaturhinweise

[1] Bundesministerium für Justiz und Verbraucherschutz, „Gesetz zur Abmilderung der Folgen der COVID-19-Pandemie im Zivil-, Insolvenz- und Strafverfahrensrecht“, https://www.bmjv.de/SharedDocs/Gesetzgebungsverfahren/Dokumente/Bgbl_Corona-Pandemie.pdf, 27.3.2020.

[2] Bundesministerium der Justiz und für Verbraucherschutz, „Verlängerung der Regelungen zur virtuellen Hauptversammlung bis Ende 2021 tritt in Kraft“, https://www.bmjv.de/SharedDocs/Pressemitteilungen/DE/2020/102920_Virtuelle_Hauptversammlung.html, 23.10.2020.

[3] The OWASP Foundation, „OWASP Top 10 – 2017“, https://owasp.org/www-project-top-ten/2017/, 2017.

[4] M. Kolšek, „Session Fixation Vulnerability in Web-based Applications“, http://www.acrossecurity.com/papers/session_fixation.pdf, 2002-2007.

[5] W. Zeller, E. W. Felten, „Cross-Site Request Forgeries: Exploitation and Prevention“, https://www.cs.utexas.edu/users/shmat/courses/library/zeller.pdf, 2008.

[6] Wappalyzer, „Wappalyzer Browser Add-On“, https://www.wappalyzer.com/, 2008-2021.

[7] S. Helme, „Security Headers“, https://securityheaders.com/, 2016-2021.

[8] Qualys Inc., „SSL Labs: SSL Server Test“, https://www.ssllabs.com/ssltest/, 2009-2021.

[9] Bundesamt für Sicherheit in der Informationstechnik, „Technische Richtlinie TR-02102-2 Kryptographische Verfahren: Empfehlungen und Schlüssellängen - Teil 2 - Verwendung von Transport Layer Security (TLS)“, https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Publikationen/TechnischeRichtlinien/TR02102/BSI-TR-02102-2.pdf, 28.2.2020.

[10] K. Moriarty, S. Farrell, „Deprecating TLSv1.0 and TLSv1.1 draft-moriarty-tls-oldversions-diediedie-01“, IETF Internet Draft, https://tools.ietf.org/id/draft-moriarty-tls-oldversions-diediedie-01.html, 25.7.2018.

[11] BSI für Bürger, „Sichere Passwörter erstellen“, https://www.bsi-fuer-buerger.de/BSIFB/DE/Empfehlungen/Passwoerter/passwoerter_node.html, online abgerufen am 31.12.2020.

[12] J. Yan, A. Salah El Ahmad, „Captcha robustness: A security engineering perspective“, Computer 44.2: 54-60, 2010.

[13] C. Danwerth, „Modalitäten und Gestaltungsvarianten der virtuellen Hauptversammlung – Eine empirische Untersuchung aller im April 2020 veröffentlichten Einberufungen präsenzloser Versammlungen von börsennotierten Unternehmen“, Die Aktiengesellschaft (AG) 2020, Heft 11: 418-432, 2020.

[14] M.Scholze, M. Kaspar, „Virtuelle Hauptversammlungen: Rückschau und Ausblick“, HV Magazin 04/2020: 12-17, 2020.

[15] Schutzgemeinschaft der Kapitalanleger e.V., „SdK fordert keine Einschränkung von Aktionärsrechten bei virtuellen Hauptversammlungen“, https://sdk.org/veroeffentlichungen/pressemitteilungen/sdk-fordert-keine-einschraenkung-von-aktionaersrechten-bei-virtuellen-hauptversammlungen/, 6.4.2020.

[16] DSW - Deutsche Schutzvereinigung für Wertpapierbesitz e.V., „Online-HV nur inklusive Aktionärsrechte“, https://www.dsw-info.de/presse/pressemitteilungen-2020/online-hv-nur-inklusive-aktionaersrechte/, 20.3.2020.