

Abschlussbericht öffentlicher Intrusionstest E-Voting

17.06.2024 – 03.07.2024

Inhaltsverzeichnis

1. Management Summary.....	2
2. Einführung.....	3
3. Durchführung PIT.....	4
3.1. Code of Conduct.....	4
3.2. Organisation.....	4
3.3. Prüfumfang.....	4
3.4. Vorbereitung eines elektronischen Urnengangs	4
3.5. Kommunikation.....	4
3.6. Teilnahmebedingungen	5
4. Ergebnisse.....	6
4.1. Befunde	6
4.2. Weitere nicht akzeptierte Befunde	7
4.3. Teilnehmende	8
4.4. Angriffe	9
5. Zusammenfassung	13

1. Management Summary

Die Post hat ihr vollständig verifizierbares System für die elektronische Stimmabgabe (E-Voting) einem öffentlichen Intrusionstest (Public Intrusion Test – PIT) unterzogen. Diese Art des Testens wird in der Fachwelt auch Penetrationstest oder kurz «Pentest» genannt. Die wiederkehrende Durchführung eines öffentlichen Intrusionstests ist eine rechtliche Vorgabe des Bundes für den E-Voting-Versuchsbetrieb¹.

Vom 17. Juni bis 03. Juli 2024 konnten ethische Hackerinnen und Hacker die E-Voting-Infrastruktur der Post angreifen. Die Interessierten testeten dabei eine exakte Kopie der produktiven Umgebung des E-Voting-Systems auf Sicherheitslücken. Dabei galten die gleichen Rahmenbedingungen, wie beim realen Einsatz von E-Voting an Wahlen und Abstimmungen. Die Fachleute konnten auch den Prozess der Stimmabgabe auf dem Abstimmungsportal mit Musterstimmrechtsausweisen 1:1 durchspielen und das System ins Visier nehmen.

Der Test wurde in der Fachszene mit Interesse aufgenommen: Es wurden von 6'923 IP-Adressen insgesamt rund 9'500 Angriffe auf das System verübt. Von 146 IP-Adressen wurden jeweils mehr als 50 Zugriffe verzeichnet. Diese werden im vorliegenden Bericht als "aktivste IP-Adresse" bezeichnet.

Es ist niemandem gelungen in das System einzudringen. Die Post hat vier Befunde erhalten und nach der Prüfung einen mit Schweregrad tief bestätigt. Der Befund betraf keine sicherheitsrelevanten Aspekte. Er zeigt eine Verbesserung in der Kommunikation zwischen den Servern auf, womit zeitgleiche Abfragen verunmöglicht werden. Die Post hat die Verbesserung im Voting-Server umgesetzt. Der Hacker hat eine Belohnung von 1'500 Franken erhalten. Als erster Hacker, der einen bestätigten Befund gemeldet hat, hat er zusätzlich einen Bonus von 3'000 Franken bekommen.

¹ Verordnung der BK über die elektronische Stimmabgabe (VEleS) vom 25. Mai 2022, Art. 10

2. Einführung

Im Rahmen ihrer Cybersecurity-Strategie lässt die Post ihre IT-Systeme öffentlich durch ethische Hackerinnen und Hacker angreifen. Bestätigte Schwachstellen belohnt sie finanziell im Rahmen von sogenannten Bug-Bounty-Programmen. Die Erfahrungen der Post zeigen, dass dies eine äusserst wirksame Methode ist, um Systeme kontinuierlich zu verbessern und gegen Angriffe zu schützen.

Die rechtlichen Grundlagen des Bundes schreiben vor, dass der Quellcode eines E-Voting-Systems dauerhaft offenzulegen ist. Zudem sollen Angriffe auf die Infrastruktur in einem ständigen Programm oder im Rahmen eines wiederkehrenden Tests mit beschränkter Laufzeit ermöglicht werden.

Die Post setzt diese Anforderungen seit 2021 um und eröffnet der Fachwelt folgende Testmöglichkeiten ihres Systems:

Unbeschränkte Laufzeit

Im Rahmen eines Community-Programms hat die Post alle wesentlichen Komponenten und Dokumente ihres E-Voting-Systems mit vollständiger Verifizierbarkeit dauerhaft offengelegt. Seit 2021 können Kryptografen und Hackerinnen den Quellcode und die Systemdokumentation auf Fehler prüfen, Angriffe simulieren und Befunde melden. Fachleute haben unterschiedliche Prüfmöglichkeiten:

- Statische Tests: Suche nach Fehlern und Schwachstellen in den veröffentlichten Dokumenten und im Quellcode der E-Voting-Software. Alle offengelegten Komponenten sind Teil dieses Tests.
- Dynamische Tests: Fachleute können das lauffähige System auf ihrer eigenen Plattform ausführen und somit Fehler im E-Voting-System inklusive den nicht direkt erreichbaren Backendsystemen ausfindig machen.

Regelmässige Durchführung mit beschränkter Laufzeit

Mit dem öffentlichen Intrusionstest bietet die Post wiederkehrend eine weitere Testmöglichkeit: Ethische Hackerinnen und Hacker können eine exakte Kopie der produktiven Umgebung des E-Voting-Systems auf Sicherheitslücken testen. Beim Test gelten damit die gleichen Rahmenbedingungen, wie beim Einsatz von E-Voting an Wahlen und Abstimmungen. Nach den Intrusionstests 2022 und 2023 wurde das vollständig verifizierbare E-Voting-System der Post vom 17.06.-03.07.2024 zum dritten Mal in einem öffentlichen Intrusionstest auf die Probe gestellt.

Der vorliegende Bericht fasst die Ergebnisse des öffentlichen Intrusionstests 2024 zusammen.

3. Durchführung PIT

3.1. Code of Conduct

Die Post hat für ihr Community-Programm zu E-Voting Verhaltensregeln für die Teilnahme definiert (Code of Conduct): Der Code of Conduct regelt den Zugang zu den Komponenten und Dokumenten des E-Voting-Systems der Post. Diese Vorgaben sind online verfügbar (<https://evoting-community.post.ch/de/code-of-conduct>).

Zusätzlich gelten für die Teilnahme am öffentlichen Bug-Bounty-Programm zu E-Voting Regeln. Auch diese sind online einsehbar (<https://yeswehack.com/programs/swiss-post-evoting>).

3.2. Organisation

Die Post führt ihre Bug-Bounty-Programme mit der unabhängigen Firma YesWeHack durch. Die YesWeHack-Plattform ist der Zugangspunkt zum Bug-Bounty-Programm und Plattform, über die ethische Hackerinnen und Hacker Befunde melden können, wenn sie dazu eine Belohnung beantragen möchten. Nach einer ersten Triage der Meldungen durch das Team von YesWeHack, analysiert ein spezialisiertes Team der Post die Befunde eingehend.

3.3. Prüfumfang

Bestandteil der Prüfung im Rahmen des öffentlichen Intrusionstests war eine exakte Kopie der produktiven Umgebung des E-Voting-Systems, in diesem Bericht als «Infrastruktur» bezeichnet. Beim Test gelten damit die gleichen Rahmenbedingungen, wie beim Einsatz von E-Voting an Wahlen und Abstimmungen

3.4. Vorbereitung eines elektronischen Urnengangs

Im Vorfeld eines realen Urnengangs erstellen die Kantone die elektronischen Urnen und generieren für alle Stimmberechtigten einen Stimmrechtsausweis. Als Systemanbieterin stellt die Schweizerische Post die Infrastruktur des E-Voting-Systems mit den Kontrollkomponenten und dem Abstimmungsportal bereit. Diese Trennung der Kompetenzen zwischen den Kantonen und der Schweizerischen Post in der Vorbereitung des elektronischen Urnengangs ist eine Sicherheitsmassnahme und eine rechtliche Vorgabe des Bundes.

Bei einem öffentlichen Intrusionstest übernimmt die Post sämtliche Vorbereitungsarbeiten und stellt den ethischen Hackerinnen und Hackern generalisierte Musterstimmrechtsausweise mit individuellen Codes, aber ohne individuelles Identifikationsmerkmal (je nach Kanton das Geburtsjahr oder Geburtsdatum) zur Verfügung.

Der elektronische Urnengang für den öffentlichen Intrusionstest wurde wie folgt definiert:

- Eine fiktive Abstimmung mit 2 Fragen
- Ein fiktiver Proporzwahlgang mit 3 Listen, 4 Kandidatinnen und Kandidaten und 2 Sitzen, die fiktiv besetzt werden können.
- Ein fiktiver Majorzwahlgang mit 5 Kandidatinnen und Kandidaten und 2 Sitzen, die fiktiv besetzt werden können.

Die Post hat 5'000 Musterstimmrechtsausweise bereitgestellt. Die Musterstimmrechtsausweise können ohne vorgängige Registrierung auf einer Webseite heruntergeladen werden.

3.5. Kommunikation

Die Post informiert die interessierten Fachleute und die Öffentlichkeit regelmässig über Neuigkeiten aus der Weiterentwicklung des Systems und über die Meldungen aus der Community. Sie veröffentlicht die bestätigten Befunde auf der Fachplattform GitLab und kommuniziert diese wie folgt:

Übersicht über die publizierten Informationen zu Befunden aus dem öffentlichen E-Voting-Bug-Bounty-Programm:

- [Results from the private bug bounty programme, 01 September 2021](#)
- [Results from the bug bounty programme, update 31 December 2021](#)
- [Results from the bug bounty programme, update 31 March 2022](#)
- [Results from the bug bounty programme, update 30 June 2022](#)
- [Results from the bug bounty programme, update 28 September 2022](#)
- [Results from the bug bounty programme, update 31 December 2022](#)
- [Results from the bug bounty programme, update 31 March 2023](#)
- [Results from the bug bounty programme, update 30 June 2023](#)
- [Results from the bug bounty programme, update 22 September 2023](#)
- [Results from the bug bounty programme, update 31 December 2023](#)
- [Results from the bug bounty programme, update 31 March 2024](#)
- [Results from the bug bounty programme, update 30 June 2024](#)

Die Post ordnet Befunde im Community-Programm in vier Schweregrade ein (tief, mittel, hoch, kritisch). Alle Befunde mit Schweregrad hoch oder kritisch beschreibt die Post nicht nur auf der Fachplattform GitLab, sondern auch auf dem E-Government-Blog für ein breiteres Publikum.

Die Post hat zum Start und im Verlauf über verschiedene Kanäle auf den öffentlichen Intrusionstest aufmerksam gemacht:

- 07.03.2024: Save-the-Date zum öffentlichen Intrusionstest über ein Mailing an die E-Voting-Fachcommunity (aufgenommen von einer Online-Fachzeitung)
- 30.05.2024: Direktnachricht via Bug-Bounty-Plattform an Researcher, die der Post bekannt sind, zur Ankündigung
- 12.06.2024: Information zum Start des öffentlichen Intrusionstests an ethische Hackerinnen und Hacker, welche dem Bug-Bounty-Programm auf der Plattform folgen mit der Anpassung der Policy auf der Bug-Bounty-Plattform
- 17.06.2024: Information zum Start des öffentlichen Intrusionstests an die Öffentlichkeit mit dem Beitrag auf dem E-Government-Blog der Post und Versand der News an einen definierten Kreis an interessierten Medien, Informationsmail an Fachcommunity und institutionelle Stakeholder, Beiträge auf den LinkedIn Accounts der Schweizerischen Post sowie auf X und LinkedIn der Partnerin der Post für das Bug-Bounty-Programm
- 26.06.2024: Beiträge auf den X- und LinkedIn Accounts der Schweizerischen Post und der Partnerin für das Bug-Bounty-Programm betreffend Bonus von 3'000 Franken zusätzlich zu den regulären Belohnungen und Information zum ersten bestätigten Befund
- 25.07.2024: Beitrag auf dem E-Government-Blog der Post zu den Ergebnissen des öffentlichen Intrusionstests

3.6. Teilnahmebedingungen

Für die Teilnahme am öffentlichen Intrusionstest ist keine Registrierung notwendig. Nur wenn jemand einen Befund über die Bug-Bounty-Plattform YesWeHack einreichen will, um eine Belohnung zu erhalten, ist eine Registrierung notwendig. Alle Kontaktdaten verbleiben bei YesWeHack und werden nicht an die Post weitergeleitet. Im Kapitel IP-Adressen nach Ländern sind die wichtigsten Zahlen zur Aktivität im öffentlichen Intrusionstest zu finden.

4. Ergebnisse

Die Post hat für den öffentlichen Intrusionstest (Scope Infrastruktur des Bug-Bounty-Programms) die Befunde mit der CVSS-Standard-Skala eingestuft (Common Vulnerability Scoring System). Diese Skala orientiert sich an einem verbreiteten Standard zur Kategorisierung von Sicherheitsbefunden.

Insgesamt hat die Post vier Befundmeldungen erhalten. Nach der Analyse konnte sie einen Befund mit Schweregrad «tief» bestätigen. Zwei andere Befunde wurden nicht bestätigt und als ‘Meldung’ geschlossen. Ein Befund wurde abgelehnt (out of scope).

Zusätzlich hat die Post während der Laufdauer des öffentlichen Intrusionstests folgende Beiträge erhalten:

- Es sind vier Meldungen zum Quellcode eingegangen. Davon konnte keine als Befund bestätigt werden. Somit wurden sie als Meldung geschlossen.
- Es sind verschiedene Vorschläge und Fragen zum E-Voting-Community-Programm eingegangen.

4.1. Befunde

Der bestätigte Befund zeigt eine Verbesserung des Voting Servers beim Verarbeiten von zeitgleichen, aber inkonsistenten Anfragen.

Titel	Die gleichzeitige Verarbeitung von verschiedenen verschlüsselten Stimmen für eine einzelne Stimmrechtsausweis-ID kann zu einem inkonsistenten Systemzustand für diese bestimmte Stimmrechtsausweis-ID führen.
Einstufung	Tief
Nummer	#YWH-PGM2323-210
Eingangsdatum	17.06.2024
Melder	Daniele Ligorio
Beschreibung	<p>Durch das gleichzeitige Durchführen mehrerer sendVote-Versuche ist es möglich, im System für eine bestimmte Stimmrechtsausweis-ID einen inkonsistenten Zustand zu induzieren, sofern der Angreifer den Initialisierungscode und den erweiterten Authentisierungsfaktor des Wählers kennt.</p> <p>Normalerweise erhält der E-Voting-Server eine verschlüsselte Stimme für eine Stimmrechtsausweis-ID und gibt diese an die vier Online-Kontrollkomponenten weiter. Um die Verfügbarkeit zu gewährleisten, verarbeitet der E-Voting-Server mehrere Anfragen parallel. Der Befund besteht darin, dass ein Angreifer viele unterschiedliche Anfragen für dieselbe Stimmrechtsausweis-ID gleichzeitig schickt. Aufgrund der parallelen Verarbeitung können unterschiedliche Anfragen an unterschiedliche Kontrollkomponenten weitergeleitet werden, was zu einem inkonsistenten Zustand des Stimmrechtsausweises führt. Das aktuelle Verhalten führt zu Time-outs, da der E-Voting-Server keine konsistente Antwort von den Kontrollkomponenten erhält.</p> <p>Diese Inkonsistenz hat keinen Einfluss auf die Verifizierbarkeit des Systems und auf das Stimmgeheimnis. Das Problem entsteht durch die zeitgleiche Verarbeitung auf dem E-Voting-Server. In unserem Bedrohungsmodell gilt der E-Voting-Server als nicht vertrauenswürdig. Für das E-Voting-System der Post muss mindestens eine Kontrollkomponente vertrauenswürdig sein. Die Kontrollkomponenten funktionieren mit einer robusten Exactly-Once-Verarbeitung und können zeitgleiche Anfragen korrekt bearbeiten.</p> <p>Zudem könnte ein Angreifer mit dem Initialisierungscode und dem erweiterten Authentisierungsfaktor den Wähler bereits an der elektronischen Stimmabgabe hindern, indem er eine Stimme abgibt, die nicht der Absicht des Wählers entspricht. Der Angreifer kann ohne Bestätigungscode die Stimme jedoch nicht bestätigen, sodass der Wähler seine Stimme weiterhin per Brief oder in einem Wahllokal abgeben kann.</p> <p>Der E-Voting-Server sollte zeitgleiche Anfragen reibungsloser behandeln und sicherstellen, dass die gleiche verschlüsselte Stimme an alle Kontrollkomponenten weitergeleitet wird.</p>
Status	In Release 1.4.3.1 haben wir erzwungen, dass der E-Voting-Server für eine einzelne Stimmrechtsausweis-ID zeitgleich nur eine Anfrage bearbeitet und allfällige weitere Anfragen ab-

	lehnt. Diese Massnahme erhöht die Robustheit des E-Voting-Servers und verhindert inkonsistente Zustände für einen bestimmten Stimmrechtsausweis im System.
Belohnung	Der Melder hat eine Belohnung von CHF 1'500.- und zusätzlich einen Bonus von CHF 3'000 erhalten, der für die Melder:innen der ersten drei bestätigten Befunde ausgeschrieben war.

4.2. Weitere nicht akzeptierte Befunde

Titel	Angeblich fehlender SPF-Eintrag ermöglicht E-Mail-Spoofing.
Nummer	#YWH-PGM2323-211
Eingangsdatum	17.06.2024
Beschreibung	Der Melder behauptet, dass ein fehlender SPF-Eintrag in der DNS-Konfiguration es Angreifern ermöglicht, E-Mails zu versenden, die scheinbar von der eigenen Domain stammen. SPF ist ein weit verbreitetes E-Mail-Validierungssystem, das diese Art von E-Mail-Spoofing erkennen und verhindern soll, indem es spezifiziert, welche E-Mail-Server E-Mails im Namen welcher Domain versenden dürfen.
Status	Als «out of scope» geschlossen. Die Post hat auf der Domain evoting.ch einen SPF-Eintrag eingerichtet. Darüber hinaus kann dieser Befund nicht als gültig angesehen werden, da er auf den nicht qualifizierenden Schwachstellen unseres Programms beruht. Phishing-Angriffe (auch bezüglich SPF/DKIM/DMARC) gelten als «out of scope».
Belohnung	Keine

Titel	Meldung zur Berücksichtigung von Gross- und Kleinschreibung im Initialisierungscode und der daraus resultierenden Entropie des abgeleiteten Codes.
Nummer	#YWH-PGM2323-212
Eingangsdatum	20.06.2024
Melder	No Breach
Beschreibung	In diesem Befund stellt der Melder infrage, ob die Entropie des Initialisierungscodes ausreichend hoch ist. Er argumentiert insbesondere, dass die Verwendung eines Alphabets, bei dem die Gross- und Kleinschreibung nicht berücksichtigt wird, für die Initialisierungscode (SVK) keinen besonderen Vorteil gegenüber einem Alphabet mit Gross- und Kleinschreibung bietet und dass im Vergleich zu Letzterem der Eingabebereich stark reduziert ist. Ein kleinerer Eingabebereich birgt ein höheres Risiko, dass zwei Wähler denselben Initialisierungscode erhalten, was Annahmen über die Eindeutigkeit der SVKs deutlich einschränken würde. Zur grösseren Sicherheit und Vermeidung von Kollisionen schlägt der Melder vor, bei Hashing-Algorithmen die Gross- und Kleinschreibung zu berücksichtigen.
Status	Als informativ geschlossen. Aufgrund des extrem grossen Umfangs des SVK-Bereichs (32^{24}) sowie der Tatsache, dass das E-Voting-System kryptografisch sichere Funktionen nutzt, um diese SVKs zufällig zu erzeugen, ist die Eindeutigkeit dieser Werte auch bei Wahlen mit einer sehr grossen Anzahl von Stimmberechtigten praktisch garantiert, und es müssen keine zusätzlichen Prüfungen durch den Verifier oder andere Instanzen durchgeführt werden, um die Generierung eines eindeutigen SVK-Wertes zu gewährleisten. Das aktuelle Alphabet ohne zusätzliche Zeichen wie Symbole und/oder Gross-/Kleinschreibung wurde bewusst gewählt für eine möglichst einfache Nutzung und um Schreibfehler so weit wie möglich vorzubeugen, sodass der Initialisierungscode von allen Bürgerinnen und Bürgern, die ihre Stimme elektronisch abgeben möchten, auf eine möglichst einfache Art und Weise verwendet werden kann. Es ist unwahrscheinlich, dass zwei Stimmberechtigte mit dem gleichen Geburtsjahr verse-

	hentlich denselben SVK erhalten, und von daher ist das Risiko einer «Kollision» vernachlässigbar. Wir weisen darauf hin, dass auch wenn der Melder den Begriff «Hash-Kollision» verwendet, das beschriebene Szenario nicht mit verschiedenen Eingaben zusammenhängt, die zu demselben Hash führen, sondern dass zwei Wähler denselben SVK erhalten, es sich also um zweimal die gleiche Eingabe handelt (die erwartungsgemäss denselben Hash erhalten würden).
Belohnung	Keine

Titel	Angebliche Race Condition auf dem Authentifizierungsendpunkt.
Nummer	#YWH-PGM2323-215
Eingangsdatum	25.06.2024
Beschreibung	<p>Der Melder behauptet, dass eine Race Condition auf dem <i>Authentifizierungsendpunkt</i> des E-Voting-Servers möglich sei und weitere Auswirkungen auf die Sicherheit haben könnte. Der Melder beschreibt weiter, dass dieses Verhalten zu potenziellen Problemen führen könnte:</p> <ul style="list-style-type: none"> • Authentisiert sich ein rechtmässiger Benutzer am System, könnte sich auch ein Angreifer authentisieren und eine Stimme vor dem Opfer abgeben. • Bei zwei Benutzern könnte es dazu kommen, dass der E-Voting-Server möglicherweise mit denselben Eingabedaten arbeitet (z. B. mit der Zeichenfolge SVK_id) und dann versucht, die Ergebnisse in der gleichen Variablen zu speichern, was zu unvorhersehbaren Ergebnissen führt.
Status	<p>Als informativ geschlossen.</p> <p>Operationen für verschiedene Benutzer laufen in getrennten Kontexten auf dem Authentifizierungsendpunkt des E-Voting-Servers. Daher konnten wir keine potenzielle Race Condition identifizieren. Darüber hinaus hat der Melder nicht konkret dargelegt, wie es zu einer solchen Wettlaufsituation kommen könnte.</p>
Belohnung	Keine

4.3. Teilnehmende

Sämtliche Domains mit dem Muster pit.evoting.ch zugeordneten IP-Adressen waren Teil des für den öffentlichen Intrusionstest definierten Scopes. Praktisch bedeutet dies, dass die ethischen Hackerinnen und Hacker den E-Voting-Server mit dem Abstimmungsportal (pit.evoting.ch) mit jeweils einer eigenen IP-Adresse angreifen konnten.

- Von rund 6'923 unterschiedlichen IP-Adressen wurde im Laufe des öffentlichen Intrusionstest mittels der Protokolle HTTP/HTTPS auf den Server pit.evoting.ch zugegriffen.
- Insgesamt wurden von 146 IP-Adressen jeweils mehr als 50 Zugriffe auf den E-Voting-Server gestellt. Diese werden als «aktivste IP-Adresse» bezeichnet.

4.3.1. IP-Adressen nach Ländern

Insgesamt konnten wir Zugriffe aus 62 Ländern feststellen. Die aktivsten IP-Adressen (> 50 Zugriffe) stammen aus insgesamt 27 Ländern. Aus den nachfolgenden Ländern verzeichnete die Post am meisten Aktivität:

Land	Anzahl IP-Adressen	Anteil
USA	28	19.2%
Schweiz	17	11.6%
Frankreich	17	11.6%
Deutschland	12	8,2%
Grossbritannien	10	6.8%
Indien	7	4.8%
Tunisien	6	4.1%
Ireland	3	2.1%
Italien	3	2.1%

Sonstige	43	29.5%
Total	146	100.0%

4.4. Angriffe

4.4.1. Anzahl der Zugriffe

Von den 6923 IP-Adressen, die insgesamt Aktivität am öffentlichen Intrusionstest verzeichnet haben, gingen insgesamt 296'172 Zugriffe auf der Domäne pit.evoting.ch ein, davon 28'977 auf dem E-Voting-Server, wovon 9'665 als Angriffe einzustufen sind.

4.4.2. Statuscodes und Anzahl der Angriffe

Für die Zugriffe sieht die Statistik mit den http-Statuscodes wie folgt aus:

Code	Code Message	Anzahl (auf pit.evoting.ch)	Anzahl (auf pit.evo- ting.ch/vote)	Anteil (auf pit.evo- ting.ch/vote)	Angriff
200	OK	34'123	13'183	38.63%	-
302	Found	229	13	5.68%	-
304	Not Modified	7'776	6'053	77.84%	-
400	Bad Request	2'160	911	42.18%	Ja
401	Unauthorized	488	488	100.00%	Ja
403	Forbidden	231'038	8'182	3.54%	Ja
404	Not Found	19'905	11	0.06%	-
408	Request Timeout	103	20	19.42%	-
500	Internal Server Error	53	51	96.23%	Ja
405 406 413 415 417 429	Method Not Allowed Not Acceptable Content Too Large Unsupported Media Type Expectation Failed Too Many Requests	264	32	12.12%	-
502	Bad Gateway	33	33	100.00%	Ja
	Gesamt	296'172	28'977	9.78%	-

Generelle Zugriffe auf die E-Voting-Infrastruktur sind in Spalte 3 aufgeführt. In Spalte 4 sind gezieltere Zugriffe auf den E-Voting-Server zu finden. Als Anzahl Angriffe sind die Fehlermeldung 400, 401, 403, 500 und 502 zusammengezählt.

Im Rahmen des Intrusionstests werden von den ethischen Hackern viele manipulierte Anfragen an den Server geschickt. Diese Anfragen werden vom Server mit einem http 400, 401, 403 oder 500 beantwortet. Die 33 Requests mit dem Statuscodes 502 «Bad Gateway» sind auf den Befund #YWH-PGM2323-210 zurückzuführen. Die Beschreibung sowie die Korrektur des Befunds sind in Kapitel 4.1 beschrieben.

4.4.3. Stimmabgabe

Die ethischen Hacker konnten auch den Prozess der Stimmabgabe auf dem Abstimmungsportal mit Musterstimmrechtsausweisen 1:1 durchspielen.

Dafür wurden insgesamt 385 Musterstimmrechtsausweisen heruntergeladen.

Die Analyse der Zugriffe der Teilnehmenden pro Prozessschritte der Stimmabgabe können wie folgt zusammengefasst werden:

Prozessschritte	Anzahl Zugriffe
Anmeldeversuche	1092
Erfolgreiche Anmeldungen	461
Fehlgeschlagene Anmeldungen	631
Erfolgreiche Stimmabgaben	189
Fehlgeschlagene Stimmabgaben	375
Erfolgreich bestätigte Stimmen	157
Fehlgeschlagene Bestätigung der Stimme	211

In realen Urnengängen gibt es meistens nur einige wenige oder gar keine fehlgeschlagenen Prozessschritte. Hier unterscheidet sich das Nutzerverhalten der Stimmberechtigten von jenem der ethischen Hackerinnen und Hacker.

4.4.4. OWASP ModSecurity Core Rule Set

Der Zugriff auf das E-Voting-System wird durch die Web Application Firewall (WAF) OWASP ModSecurity Core Rule Set 3 (CRS) geschützt. Das CRS ist auf Paranoia Level 4 konfiguriert, der höchsten Schutzstufe, welche in dem Regelwerk verfügbar ist. Während mehreren Jahren hat die Schweizerische Post eine Feinabstimmung der CRS-Installation und des Regelwerks vorgenommen.

Insgesamt wurden 8'194 Zugriffe aufgrund von Warnmeldungen blockiert, welche durch das CRS ausgelöst wurden. Einige der Warnmeldungen wurden ignoriert, da sie unter einer bestimmten Wertgrenze (Ungewöhnlichkeitsschwelle) lagen.

Die Post unterstützt als Sponsorin das Cybersecurity-Framework OWASP Core Rule Set. OWASP CRS in Verbindung mit Apache ModSecurity, ist eine der wirksamsten IT- Abwehrlösungen, die heute verfügbar sind. OWASP CRS ist eine Open-Source-Lösung. Mit dem Sponsoring unterstützt die Post die Stiftung und damit ein Abwehrsystem, das hilft, Cybersecurity weltweit zu stärken.

4.4.5. ModSecurity Allow List

Damit das CRS Regelwerk nicht im generellen alle Zugriffe abblockt, müssen gewisse Werte und Parameter auf eine Liste (Whitelist) gesetzt werden. Diese Liste bestimmt, welche Abfragen erlaubt sind.

Bei der Allow-List handelt es sich um ein zweites, komplementäres Regelwerk, das gemeinsam mit CRS zum Einsatz kommt. In diesem Regelwerk werden ähnlich wie bei einer Netzwerk-Firewall sämtliche Zugriffe verboten und nur eine klar definierte Liste von erlaubten Zugriffen darf auf den Server erfolgen.

- Der Zugriff eines Endbenutzers auf das E-Voting-System ist durch eine benutzerdefinierte Allow List geschützt, die API-Endpunkte (URIs), Parameter und bestimmte andere Merkmale der Zugriffe abdeckt.
- Es ist technisch möglich, dass ein Zugriff eine oder mehrere CRS- und Allow-List-Regeln auslöst, bevor sie schliesslich blockiert oder auf einen verschlüsselten Port des Dienstes weitergeleitet wird. Die Zahlen aus dem vorherigen Abschnitt stimmen daher nicht mit den hier vorgestellten Zahlen überein.
- Insgesamt wurden 185'733 Zugriffe aufgrund von Allow List-Verstössen blockiert.

4.4.6. ModSecurity Javascript Hash Check

Eine weitere Schutzmassnahme ist der Hash Check. Für jede Datei auf einem Computer kann eine eindeutige Prüfzahl (Hash) berechnet werden. Sobald eine Änderung an der Datei vorgenommen wird, verändert sich diese Zahl. Beim Hash Check wird die Prüfzahl der an den Abstimmungsclient zurück gesendeten Datei mit der vorgängig errechneten und in der ModSecurity Konfiguration der Web Application Firewall eingepflegten Prüfzahl verglichen, um Manipulationen auf dem E-Voting-Server zu erkennen. Mit dieser Sicherheitsprüfung soll der Schutz der Abstimmung vor internen Angreifern gewährleistet werden.

Es gab keine Anzeichen für einen möglichen internen Angriff.

Wichtig: Das E-Voting-System der Post ermöglicht auch den Nutzerinnen und Nutzern zu prüfen, bei einem realen Urnengang also den Stimmberechtigten, dass die richtigen HTML und JavaScript Dateien geschickt wurden². Es gab keine Meldungen, dass diese Prüfung fehlgeschlagen wäre.

4.4.7. Zusätzliche Sicherheitsmassnahmen

Das E-Voting-System verfügt über zusätzliche Sicherheitsmassnahmen, welche das Risiko weiter minimieren, dass ein externer Angreifer den E-Voting-Server erreicht. Für den öffentlichen Intrusionstest wurden diese Massnahmen nicht aktiviert.

Beispiel für eine weitere Schutzmassnahme ist die Fail2ban-Konfiguration, welche eine IP-Adresse nach einer bestimmten Anzahl falscher Zugriffe für eine definierte Zeit blockiert. Diese Konfiguration verhindert einen Angriff nicht grundsätzlich, erschwert jedoch das Eindringen weiter.

Wäre die gleiche Konfiguration bei einem produktiven Urnengang der Kantone zum Einsatz gekommen, wären 39 % des beim öffentlichen Intrusionstest registrierten Netzwerkverkehrs zum E-Voting-Server durch die aktive Steuerung/Begrenzung des Datenverkehrs blockiert worden. Um die Zugangsbarriere für die Fachexperten niedrig zu halten, hat die Post dieses Filtersystem in den Simulationsmodus versetzt bzw. deaktiviert.

² <https://gitlab.com/swisspost-evoting/e-voting/e-voting-documentation/-/blob/master/Security-advice/de/readme.md#hashwerte-%C3%BCberpr%C3%BCfen-erweiterte-pr%C3%BCfung>

4.4.8.mod_qos

Das Modul mod_qos wird zur Abwehr von DoS-Angriffen eingesetzt. Damit sollen aggressive Scanning Aktivitäten verlangsamt werden, da diese eine Bedrohung für die Verfügbarkeit des E-Voting-Systems darstellen könnten. Bezüglich Scanning in der produktiven E-Voting-Umgebung gilt eine Nulltoleranz, und sämtliche erkannten Scanning Aktivitäten würden unmittelbar gestoppt.

In der folgenden Auflistung sind die Anzahl an gesperrten Zugriffen pro Datum aus dem öffentlichen Intrusionstest ersichtlich:

Datum	Anzahl
2024-06-12	0
2024-06-13	0
2024-06-14	3
2024-06-15	17
2024-06-16	5
2024-06-17	55
2024-06-18	0
2024-06-19	3
2024-06-20	6
2024-06-21	0
2024-06-22	0
2024-06-23	0
2024-06-24	0
2024-06-25	0
2024-06-26	0
2024-06-27	3
2024-06-28	1
2024-06-29	1
2024-06-30	1
2024-07-01	7
2024-07-02	9
2024-07-03	1

5. Zusammenfassung

Nachstehend findet sich eine Zusammenfassung zu den wichtigsten Ergebnissen aus dem öffentlichen Intrusionstest zum vollständig verifizierbaren E-Voting-System der Post vom 17.06.-03.07.2024:

- **Teilnahme:** Es haben rund 6'923 IP-Adressen am öffentlichen Intrusionstest teilgenommen. Insgesamt hat die Post 146 IP-Adressen mit mehr als 50 Zugriffen von der gleichen IP-Adresse auf den E-Voting-Server verzeichnet. 19.2 Prozent dieser «aktivsten IP-Adressen» stammt aus die Vereinigten Staaten von Amerika, gefolgt von der Schweiz und Frankreich mit jeweils 11.6%. Im Vergleich zu 2022 und 2023 haben mehr IP-Adressen teilgenommen, die Anzahl der «aktivsten IP-Adressen» war jedoch tiefer.
- **Kommunikationsmassnahmen:** Die Post hat über verschiedene Kanäle aktiv zum öffentlichen Intrusionstest kommuniziert. Sie hat Informationen im Vorfeld, zum Start und während dem Verlauf des Tests verschickt (via Bug Bounty Plattform, E-Government-Blog, Mailings an Fachcommunity und institutionelle Stakeholder, Beiträge auf den X- und LinkedIn Accounts der Schweizerischen Post und der Partnerin für das Bug-Bounty-Programm).
- **Angriffe:** Mit 6'923 unterschiedlichen IP-Adressen wurde im Zuge des öffentlichen Intrusionstest mittels der Protokolle HTTP/HTTPS insgesamt über 296'000 mal auf pit.evoting.ch zugegriffen. Rund 29'000 Zugriffe gingen auf dem Abstimmungsportal pit.evoting.ch/vote ein, wovon 9'665 als Angriffsversuche einzustufen.
- **Befunde:** Es ist den Teilnehmenden nicht gelungen, in das System einzudringen. Die Post hat vier Befunde erhalten, davon hat sie einen bestätigt. Der Befund betraf keine sicherheitsrelevanten Aspekte. Er zeigt eine Verbesserung in der Kommunikation zwischen den Servern auf, womit zeitgleiche Abfragen verunmöglicht werden. Die Post hat die Verbesserung im Voting-Server umgesetzt. Die Einstufung des Schweregrades ist «tief». Der Melder erhält für den Befund eine Belohnung von 1'500 Franken und zusätzlich einen Bonus von 3'000 Franken. Die Post hat den Befund bereits behoben.

Der öffentliche Intrusionstest deckte trotz einer breiten Beteiligung von ethischen Hackern keine Sicherheitslücken auf und brachte die operativen Systeme zu keiner Zeit an die Belastungsgrenzen. Die IT-Sicherheitsanalysen zeigen, dass die Sicherheitsstandards der Schweizerischen Post alle Angriffsversuche abwehren konnten.