

# E-Voting-System: Abschlussbericht öffentlicher Intrusionstest 08.08.-02.09.2022

## Inhalt

<b>1. Management Summary</b>	<b>2</b>
<b>2. Einführung</b>	<b>3</b>
<b>3. Vorbereitende Arbeiten</b>	<b>4</b>
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
<b>4. Ergebnisse</b>	<b>6</b>
4.1. Befunde	6
4.2. Teilnehmende	7
4.2.1. pit.evoting.ch	7
4.2.2. pit-admin.evoting.ch	7
4.2.3. IP-Adressen nach Ländern	7
4.3. Angriffe	8
4.3.1. Anzahl der Zugriffe	8
4.3.2. Statuscodes und Anzahl der Angriffe	8
4.3.3. Stimmabgabe	8
4.3.4. OWASP ModSecurity Core Rule Set	8
4.3.5. ModSecurity Allow List	9
4.3.6. ModSecurity Javascript Hash Check	9
4.3.7. Zusätzliche Sicherheitsmassnahmen	9
4.3.8. mod_qos	9
<b>5. Fazit</b>	<b>11</b>

## Änderungskontrolle

Diese Seite zeigt den Änderungsstand dieses Dokumentes. Mit jeder Änderung erfolgt eine Neuausgabe

Version	Ersteller	Datum
1.0	Swiss Post e-voting team	27.09.2022

## 1. Management Summary

Die Post hat zu ihrem System für die elektronische Stimmabgabe (E-Voting) einen öffentlichen Intrusionstest (Public Intrusion Test – PIT) durchgeführt. Diese Art des Testens wird in der Fachwelt auch Penetrationstest oder kurz «Pentest» genannt. Die wiederkehrende Durchführung eines öffentlichen Intrusionstests ist eine rechtliche Anforderung des Bundes für den E-Voting-Versuchsbetrieb<sup>1</sup>.

Während vier Wochen, vom 8. August bis am 2. September 2022, konnten ethische Hackerinnen und Hacker die E-Voting-Infrastruktur der Post angreifen. Die Interessierten konnten dabei diejenige Infrastruktur testen, welche zukünftig für den Einsatz des Systems an Wahlen und Abstimmungen vorgesehen ist. Die ethischen Hacker 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 3400 IP-Adressen insgesamt mehr als 60'000 Angriffe auf das System verübt. Von 178 der verzeichneten IP-Adressen wurden jeweils mehr als 50 Zugriffe versucht. Diese werden im vorliegenden Bericht als "aktivste Teilnehmende" bezeichnet.

Es ist keinem Hacker gelungen in das System einzudringen. Die Post hat zwei Befunde erhalten und nach der Prüfung einen mit Schweregrad tief bestätigt.

Der bestätigte Befund betrifft keine sicherheitsrelevanten Aspekte, hilft aber, Prozesse auf dem Abstimmungsportal zu verschlanken. Die Post wird diese Verbesserung im Sinne einer Best Practice umsetzen und hat dem ethischen Hacker eine Belohnung von CHF 500.- ausbezahlt.

Der zweite Befund betraf die Applikation zum Download eines Musterstimmrechtsausweises, den die Post für den öffentlichen Intrusionstest bereitgestellt hat, damit die Hacker den Vorgang der elektronischen Stimmabgabe durchspielen konnten. Bei einem realen Urnengang laden die Stimmberechtigten die Stimmrechtsausweise nicht selbst herunter, sondern erhalten diese per Post. Dieser Befund lag entsprechend ausserhalb des definierten Prüfbereichs des öffentlichen Intrusionstests und wurde deshalb nicht bestätigt.

Der erfolgreiche Abschluss des öffentlichen Intrusionstests gemäss den Vorgaben des Bundes für den E-Voting-Versuchsbetrieb ist damit auch ein weiterer Schritt hin zur Bereitstellung des Systems.

---

<sup>1</sup> 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 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 Post hat im Rahmen eines Community-Programms alle wesentlichen Komponenten und Dokumente ihres zukünftigen E-Voting-System mit vollständiger Verifizierbarkeit dauerhaft offengelegt. Seit 2021 können Kryptografen und Hackerinnen den Quellcode und die Systemdokumentation auf Fehler prüfen und Angriffe simulieren. Mit dem öffentlichen Intrusionstest hat die Post die Testmöglichkeiten erweitert: Während vier Wochen, vom 8. August bis am 2. September 2022, konnten ethische Hackerinnen und Hacker die E-Voting-Infrastruktur der Post angreifen. Die Interessierten trafen dabei 1:1 auf die Infrastruktur, die für den Einsatz des Systems bei Wahlen und Abstimmungen vorgesehen ist. Die ethischen Hacker konnten zudem erstmals auf dem zukünftigen E-Voting-System den Prozess der Stimmabgabe auf dem Abstimmungsportal mit Musterstimmrechtsausweisen durchspielen und das System ins Visier nehmen.

Die rechtlichen Grundlagen des Bundes schreiben vor, dass der Quellcode eines E-Voting-Systems dauerhaft offengelegt werden muss. Zudem sollen Angriffe auf die Infrastruktur in einem ständigen Programm oder als einem wiederkehrenden Test mit beschränkter Laufzeit ermöglicht werden.

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

### **Dauerhaft, ohne zeitliche Begrenzung**

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

### **Regelmässige Durchführung, jeweils zeitlich begrenzt**

Öffentlicher Intrusionstest: Angriffe auf das 1:1 System und Versuch, in die elektronische Infrastruktur einzudringen

Die Post lanciert ihre Bug-Bounty-Programme stufenweise, d.h. sie startet mit einer Gruppe von Fachleuten und erweitert diesen Kreis kontinuierlich, bis sie ein Programm öffnet, alle Interessierten dazu einlädt und die Öffentlichkeit darüber informiert. Dieses stufenweise Vorgehen ist in der Branche für die Zusammenarbeit mit ethischen Hackern üblich.

Für das E-Voting-System hat die Post 2021 ein Bug-Bounty-Programm mit einer begrenzten Gruppe von Hackern gestartet («privates Programm»). Die Teilnehmenden konnten alle wesentlichen Systemkomponenten und -dokumentationen prüfen und auch die Infrastruktur angreifen. Aus diesem «privaten Intrusionstest» sind bis August 2021 sieben bestätigte Befunde eingegangen.

Im Zeitraum vom 08.08. bis 02.09.2022 hat die Post den öffentlichen Intrusionstest durchgeführt und ethischen Hackern ermöglicht, die Infrastruktur mit Angriffen auf die Probe zu stellen. Eine Periode von 4 Woche entspricht der in den meisten Kantonen üblichen Dauer eines Urnengangs (Zeitdauer vom Versand der Abstimmungsunterlagen bis zur Auszählung der Stimmen). Die Post möchte die Tests 1:1 auf der Infrastruktur durchführen, die für den Einsatz in den Kantonen vorgesehen ist. Damit keine Abstimmungen gestört werden, ist dies nur möglich, wenn ein begrenztes Testfenster zur Verfügung steht.

Der vorliegende Bericht fasst die Ergebnisse dieses öffentlichen Intrusionstests zusammen.

### 3. Vorbereitende Arbeiten

#### 3.1. Code of Conduct

Die Post hat für ihr Community Programm 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. Der Code of Conduct zum Community-Programm ist 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 die Meldestelle für Findings. Nach einer ersten Triage der eingehenden Meldungen durch das Team von YesWeHack, hat sich ein spezialisiertes Team der Post um die Analyse der Befunde gekümmert.

#### 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» referenziert. Die Post hat dafür 1:1 die Infrastruktur bereitgestellt, die für den Einsatz des Systems bei Wahlen und Abstimmungen vorgesehen ist.

#### 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 Post die Infrastruktur des E-Voting-Systems mit den Kontrollkomponenten und dem Abstimmungsportal bereit.

Diese Kompetenzentrennung zwischen den Kantonen und des Systemanbieters (Der Schweizerischen Post) in der Vorbereitung des elektronischen Urnengangs ist eine Sicherheitsmassnahme und eine rechtliche Vorgabe des Bundes.

Für das Test-Setting, d.h. für den öffentlichen Intrusionstest, hat die Post sämtliche Vorbereitungsarbeiten, d.h. die Bereitstellung der Urnen, der Stimmrechtsausweise und der E-Voting-Infrastruktur, übernommen.

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

- Eine fiktive, eidgenössische Abstimmung, kein Wahlgang
- Die beiden Abstimmungsfragen wurden neutral formuliert. Sie konnten mit JA, NEIN oder LEER beantwortet werden.
- Es wurden 5'000 Musterstimmrechtsausweise bereitgestellt, damit die Hacker die elektronische Stimmabgabe 1:1 durchspielen könnten.

Die Musterstimmrechtsausweise konnten ohne vorgängige Registrierung via eine dedizierte Webseite bezogen 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.

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](#)

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 zusätzlich auf dem [E-Voting-Blog](#) für ein breiteres Publikum.

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

- Verteilung von Flyer anlässlich der Le Hack in Paris (25./26.06.2022)
- 08.08.2022: Medienmitteilung, E-Voting-Blog-Beitrag, Newsmail an die E-Voting-Community
- 18.08.2022: Medienblog mit einem Interview mit einem ethischen Hacker
- Verschiedene Aktivitäten auf Social Media, darunter Tweets auf den Twitterkanälen der Post und der Plattformbetreiberin YesWeHack

### **3.6. Teilnahmebedingungen**

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

## 4. Ergebnisse

### 4.1. Befunde

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)<sup>2</sup>. Diese Skala orientiert sich an einem verbreiteten Standard zur Kategorisierung von Sicherheitsbefunden.

Insgesamt hat die Post zwei Befundmeldungen erhalten. Nach der Analyse der Befunde konnte sie einen Befund mit Schweregrad «tief» bestätigen. Der zweite Befund lag nicht im Prüfumfang des öffentlichen Intrusionstests.

Der bestätigte Befund zeigt auf, dass Prozesse auf dem Abstimmungsportal verschlankt werden können. Der Befund ist nachstehend beschrieben.

<b>Inaktive Stimmrechtsausweise können verwendet werden, um die Wahlmöglichkeiten offen zu legen</b>	
<b>Titel</b>	
<b>Einstufung</b>	<b>Tief</b>
<b>Nummer</b>	#YWH-PGM2323-92
<b>Eingangsdatum</b>	02.09.2022
<b>Melder</b>	Dharmaraj PS
<b>Beschreibung</b>	<p>Wenn eine Person mit böswilligen Absichten an einen ungültigen Stimmrechtsausweis kommt, z.B. von einer Person, die schon abgestimmt hat, kann sie mittels Manipulation das Abstimmungsportal dazu bringen, für den Prozessschritt nicht benötigte, aber nicht-sensible Informationen anzuzeigen. Im Backend des Abstimmungsportals wird nicht nur die Meldung übermittelt, dass der Stimmrechtsausweis deaktiviert ist, sondern es werden auch die Wahloptionen, die auf dem Stimmzettel zu finden sind, mitübermittelt.</p> <p>Ein Onlinesystem sollte nur die notwendigen Informationen weitergeben - und nicht mehr. Die Antwort des Backends sollte nicht den Inhalt des Stimmrechtsausweises wiedergeben.</p>
<b>Status</b>	<p>Alle vorgedruckten Inhalte des Wahlzettels sind öffentlich, daher handelt es sich nicht um sensible Informationen und es besteht keinerlei Risiko für die Sicherheit oder Vertraulichkeit der elektronischen Stimmabgabe. Dieser Befund wurde als Best Practice eingestuft.</p> <p>Die Post hat den Befund bestätigt und wird die Verbesserung im System vornehmen.</p>
<b>Belohnung</b>	Der Melder hat eine Belohnung von CHF 500.- erhalten.

Der zweite gemeldete Befund betraf die Applikation zum Download eines Musterstimmrechtsausweises, den die Post für den öffentlichen Intrusionstest bereitgestellt hat, damit die Hacker den Vorgang der elektronischen Stimmabgabe durchspielen konnten. Bei einem realen Urnengang laden die Stimmberechtigten die Stimmrechtsausweise nicht selbst herunter, sondern erhalten diese per Post. Dieser Befund lag entsprechend ausserhalb des definierten Prüfbereichs des öffentlichen Intrusionstests.

Weiterführende Informationen zu den Befunden, die während dem öffentlichen Intrusionstest zu den übrigen Prüfbereichen (Scopes) im E-Voting-Community-Programm eingegangen sind, finden sich auf:

– [Results from the bug bounty programme, update 28 September 2022](#)

<sup>2</sup> [Common Vulnerability Scoring System Version 3.1 Calculator \(first.org\)](#)

## 4.2. Teilnehmende

Die Post hat für den öffentlichen Intrusionstest einen Test-Urnengang auf der 1:1 Infrastruktur vorbereitet, die für den Einsatz vorgesehen ist und diesen wie einen realen Urnengang aufgebaut.

Sämtliche den 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 Hacker den E-Voting-Server mit dem Abstimmungsportal (pit.evoting.ch) und das kantonale Administrationsportal (pit-admin.evoting.ch) mit jeweils einer eigenen IP-Adresse angreifen konnten.

### 4.2.1.pit.evoting.ch

- Von rund 3'400 unterschiedlichen IP-Adressen wurde im Laufe des öffentlichen Intrusionstest mittels der Protokolle HTTP/HTTPS auf den Server pit.evoting.ch zugegriffen.
- Von 61 IP-Adressen wurde versucht, über pit.evoting.ch Stimmen abzugeben.
- Von 58 IP-Adressen wurde mindestens eine Stimme erfolgreich abgegeben.
- Insgesamt wurden von 178 IP-Adressen jeweils mehr als 50 Zugriffe auf den E-Voting-Server gestellt. Diese werden als «aktivste Teilnehmende» bezeichnet.

### 4.2.2.pit-admin.evoting.ch

Von 389 unterschiedliche IP-Adressen gingen während des öffentlichen Intrusionstests Zugriffe mittels HTTP/HTTPS auf das Administrationsportal aus.

Das Administrationsportal erlaubt Zugriffe nur dann, wenn ein gültiges Client-Zertifikat zur Authentifizierung verwendet wird. In der Folge gelang kein einziger erfolgreicher Zugriff auf das Administrationsportal. Stattdessen wurden die Zugriffe vom System erkannt und als unzulässige Zugriffe blockiert. Der Rest dieses Berichts konzentriert auf den E-Voting-Server (Abstimmungsportal).

### 4.2.3.IP-Adressen nach Ländern

Unter den aktivsten IP-Adressen (> 50 Zugriffe) sind die nachfolgenden Länder am stärksten vertreten:

Land	Anzahl IP-Adressen	Anteil
Schweiz	48	26,97%
USA	34	19,10%
Deutschland	17	9,55%
Niederlanden	13	7,30%
Frankreich	11	6,18%
Tunesien	11	6,18%
Russland	6	3,37%
Indien	5	2,81%
Grossbritannien	4	2,25%
China	3	1,69%
Singapur	3	1,69%
Australien	2	1,12%
Belgien	2	1,12%
Tschechische Republik	2	1,12%
Spanien	2	1,12%
Ukraine	2	1,12%
Sonstige	13	7,31%
Total	178	100,00%

### 4.3. Angriffe

#### 4.3.1. Anzahl der Zugriffe

- Von den 3400 IP-Adressen, die insgesamt Aktivität am öffentlichen Intrusionstest verzeichnet haben, gingen 3'781'240 Zugriffe aus.
- Von den 178 IP-Adressen, die im öffentlichen Intrusionstest am meisten Aktivität verzeichnet haben, gingen insgesamt 150'125 Zugriffe auf den E-Voting-Server aus.
- Dies bedeutet, dass durchschnittlich 843 Zugriffe mit einem Medianwert von 112 Zugriffen pro IP-Adresse erfolgt sind.

#### 4.3.2. Statuscodes und Anzahl der Angriffe

Für die 150'125 Zugriffe sieht die Statistik mit den http-Statuscodes wie folgt aus:

Code	Code Message	Anzahl	Anteil	Angriff
200	OK	73'479	48,95%	
301	Moved Permanently	7'821	5,21%	
304	Not Modified	482	0,32%	
400	Bad Request	1'221	0,81%	1'221
403	Forbidden	61'796	41,16%	61'796
404	Not Found	4'435	2,95%	
408	Request Timeout	819	0,55%	
500	Internal Server Error	72	0,05%	72
Gesamt		150'125	100,00%	63'089

Das Fehlen des Statuscode 502 «Bad Gateway» deutet auf eine gute Verfügbarkeit der Back-End-Systeme hin.

Die 72 Zugriffe, welche zum Statuscode 500 «Internal Server Error» geführt haben, sind auf falsch codierte Zugriffe an den Server zurückzuführen. Im öffentlichen Intrusionstest wurden keine Befunde gemeldet, welche Bezug auf den Statuscode 500 genommen hätten.

#### 4.3.3. Stimmabgabe

Die ethischen Hacker konnten auch den Prozess der Stimmabgabe auf dem Abstimmungsportal mit Musterstimmrechtsausweisen, analog einem/r zukünftigen Stimmbürger/in, 1:1 durchspielen.

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

Prozessschritte	Anzahl Zugriffe
Anmeldeversuche	1'706 von 98 unterschiedlichen IP-Adressen
Erfolgreiche Anmeldungen	332 von 85 unterschiedlichen IP-Adressen
Fehlgeschlagene Anmeldungen	1'374 von 44 unterschiedlichen IP-Adressen
Erfolge mit Authentisierungstoken	228 von 79 unterschiedlichen IP-Adressen
Fehlversuche mit Authentisierungstoken	14 von 4 unterschiedlichen IP-Adressen
Erfolgreiche Stimmabgaben	82 von 59 unterschiedlichen IP-Adressen
Fehlgeschlagene Stimmabgaben	7 von 3 unterschiedlichen IP-Adressen
Erfolgreich bestätigte Stimmen	79 von 58 unterschiedlichen IP-Adressen
Fehlgeschlagene Bestätigung der Stimme	12 von 3 unterschiedlichen IP-Adressen

In einem realen Urnengang ist die Anzahl fehlgeschlagener Zugriffe deutlich tiefer als im durchgeführten Intrusionstest.

#### 4.3.4. 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. Es waren daher nur sehr wenige Falschmeldungen zu verzeichnen.

Insgesamt wurden 53'537 Zugriffe aufgrund von Warnmeldungen blockiert, welche durch das CRS ausgelöst wurden. Einige der Warnmeldungen wurden ignoriert, da sie unter einer bestimmten Wertgrenze (Ungewöhnlichkeitsschwelle) lagen.

#### 4.3.5.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 im generellen 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 zugreifen.

- 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 65'666 Zugriffe aufgrund von Allow List-Verstössen blockiert.

#### 4.3.6.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 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.

- Die an die Abstimmungsclients zurückgegebenen Javascript-Dateien werden auf dem Weg zum Client auf ihre Konsistenz hin überprüft. Mit dieser Sicherheitsprüfung soll der Schutz der Abstimmung vor internen Angreifern gewährleistet werden.
- 4'323 Zugriffe durchliefen diese Prüfung erfolgreich.
- Zu beachten ist, dass in Bezug auf dieses mögliche Fehlverhalten keine Meldung eingegangen ist.

#### 4.3.7.Zusätzliche Sicherheitsmassnahmen

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

Beispiel für eine weitere Schutzmassnahme ist die Fail2ban-Konfiguration, welche eine IP-Adresse nach bestimmter Anzahl falscher Zugriffe für eine bestimmte Zeit blockiert. Diese Konfiguration verhindert einen Angriff nicht grundsätzlich, erschwert jedoch das Eindringen durch Verzögerungsmassnahmen.

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, wurde unser Filtersystem in den Simulationsmodus versetzt bzw. deaktiviert.

#### 4.3.8.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:

<b>Datum</b>	<b>Anzahl</b>
08.08.2022	1'545
09.08.2022	32
11.08.2022	32
15.08.2022	59
17.08.2022	32
19.08.2022	32
20.08.2022	64
21.08.2022	66
22.08.2022	60
25.08.2022	21
26.08.2022	32
27.08.2022	32
29.08.2022	81
01.09.2022	96

## 5. Fazit

Nachstehend findet sich eine Zusammenfassung zu den wichtigsten Ergebnissen aus dem öffentlichen Intrusionstest zum E-Voting-System der Post vom 08.08.-02.09.2022:

- **Teilnehmende:** Es haben 3'400 Personen (IP-Adressen) am öffentlichen Intrusionstest teilgenommen. Geografisch stammen die meisten Anfragen von IP-Adressen aus den USA und China. Insgesamt hat die Post 178 IP-Adressen mit mehr als 50 Zugriffen auf den E-Voting-Server verzeichnet. Gut ein Viertel dieser «aktivsten Teilnehmenden» stammt aus der Schweiz, rund 20 Prozent aus den USA und 10 Prozent aus Deutschland.
- **Befunde:** Die Post hat zwei Befunde erhalten. Davon hat sie einen bestätigt. Es handelt sich um eine Best Practice (Schweregrad tief) und betrifft eine Verbesserung zur Verschlankung der Prozesse auf dem Abstimmungsportal. Die Post setzt die Verbesserung um Befund und hat dem Melder eine Belohnung von CHF 500.- ausbezahlt. Der zweite Befund betraf die Applikation zum Download eines Musterstimmrechtsausweises, den die Post für den öffentlichen Intrusionstest bereitgestellt hat, damit die Hacker den Vorgang der elektronischen Stimmabgabe durchspielen konnten. Bei einem realen Urnengang laden die Stimmberechtigten die Stimmrechtsausweise nicht selbst herunter, sondern erhalten diese per Post. Dieser Befund lag entsprechend ausserhalb des definierten Prüfbereichs des öffentlichen Intrusionstests.
- **Angriffe:** Mit rund 3'400 unterschiedlichen IP-Adressen wurde im Zuge des öffentlichen Intrusionstest mittels der Protokolle HTTP/HTTPS insgesamt über 3.7 Mio. mal auf den E-Voting-Server zugegriffen. Von 389 unterschiedlichen IP-Adressen wurde mittels HTTP/HTTPS auf das kantonale Administrationsportal zugegriffen. Die 178 aktivsten Teilnehmenden griffen insgesamt 150'125-mal auf die E-Voting-Server zu, wovon über 60'000 als Angriffe einzustufen sind.

Der öffentliche Intrusionstest deckte trotz einer breiten Beteiligung von etischen 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 innerhalb des gesteckten Rahmens abwehren konnten.