

Abschlussbericht öffentlicher Intrusionstest E-Voting

08.07.2023 - 31.07.2023

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	9
4.4. Angriffe.....	10
5. Zusammenfassung.....	14

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-Versuchsbetrieb¹.

Vom 8. Juli bis 31. Juli 2023 konnten ethische Hackerinnen und Hacker die E-Voting-Infrastruktur der Post angreifen. Die Interessierten konnten dabei diejenige Infrastruktur testen, welche 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 2650 IP-Adressen insgesamt mehr als 53'000 Angriffe auf das System verübt. Von 273 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 vier Befunde erhalten und nach der Prüfung einen mit Schweregrad tief bestätigt. Der Befund betraf keine sicherheitsrelevanten Aspekte und zeigt eine Verbesserung der Reverse Proxy Konfiguration in der E-Voting Webinfrastruktur auf. Die Post hat diese Verbesserung bereits umgesetzt. Der Hacker hat eine Belohnung von 1000 Franken erhalten. Als erster Hacker, der einen bestätigten Befund meldete, hat er zusätzlich einen Bonus von 3000 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 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.

Für E-Voting schreiben die rechtlichen Grundlagen des Bundes vor, dass der Quellcode eines E-Voting-Systems dauerhaft offenzulegen ist. 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:

Unbeschränkte Laufzeit

Die Post hat im Rahmen eines Community-Programms alle wesentlichen Komponenten und Dokumente ihres neuen 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 finden.

Regelmässige Durchführung mit beschränkter Laufzeit

Mit dem öffentlichen Intrusionstest bietet die Post wiederkehrend eine weitere Testmöglichkeit: Ethische Hackerinnen und Hacker können das System in der 1:1 Infrastruktur angreifen. Sie treffen dabei auf die gleiche Infrastruktur, welche die Post beim Einsatz des Systems an realen Wahlen und Abstimmungen bereitstellt. Nach dem letztjährigen Intrusionstest im Herbst 2022 fand im Juli 2023 ein erneuter öffentlicher Intrusionstest statt.

Der vorliegende Bericht fasst die Ergebnisse des öffentlichen Intrusionstests 2023 zusammen.

3. Durchführung PIT

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» bezeichnet. 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 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.

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

- Ein fiktiver Wahlgang mit 5 Listen, 23 Kandidatinnen und Kandidaten und 5 Sitze, die fiktiv besetzt werden können.
- Die Post hat 5'000 Musterstimmrechtsausweise bereitgestellt, damit die Hacker die elektronische Stimmabgabe 1:1 durchspielen könnten.

Die Musterstimmrechtsausweise konnten 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](#)

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-Voting-Blog](#) für ein breiteres Publikum.

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

- 14.06.2023: Direktnachricht via Bug-Bounty-Plattform an Researcher, die der Post bekannt sind, zur Ankündigung
- 07.07.2023: Direktnachricht via Bug-Bounty-Plattform an bekannte Researcher als Reminder zum bevorstehenden Start
- 12.07.2023: Beitrag auf dem E-Voting-Blog und Versand der News an einen definierten Kreis an interessierten Medien, Informationsmail an Fachcommunity und institutionelle Stakeholder, politischer Newsletter, Beiträge auf den Twitter- und LinkedIn Accounts der Schweizerischen Post und der Partnerin für das Bug-Bounty-Programm
- 19.07.2023: Beiträge auf den Twitter- und LinkedIn Accounts der Schweizerischen Post und der Partnerin für das Bug-Bounty-Programm betreffend Bonus von €3'000 zusätzlich zu den regulären Belohnungen für die ersten drei Melder eines bestätigten Befundes
- 27.07.2023: Interview mit dem ersten Melder eines bestätigten Befundes auf dem E-Voting-Blog, Beiträge auf den Twitter- und LinkedIn Accounts der Schweizerischen Post und der Partnerin für das Bug-Bounty-Programm zum Interview und zu den verbleibenden 5 Tagen des Intrusionstests
- 16.08.2023: Beitrag auf dem Medienblog der Schweizerischen Post zu den Ergebnissen des öffentlichen Intrusionstests

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). Diese Skala orientiert sich an einem verbreiteten Standard zur Kategorisierung von Sicherheitsbefunden.

Insgesamt hat die Post vier Befundmeldungen erhalten. Nach der Analyse der Befunde konnte sie einen Befund mit Schweregrad «tief» bestätigen. Die andere drei Befunde wurden nicht bestätigt und als 'Meldung' geschlossen.

Der bestätigte Befund zeigt eine Verbesserung der Reverse Proxy Konfiguration in der E-Voting Infrastruktur auf.

Titel	Reverse-Proxy validiert Eingaben in einem bestimmten Fall unzureichend, wenn Anfragen an einen anderen Ort umgeleitet werden.
Einstufung	Tief
Nummer	#YWH-PGM2323-187
Eingangsdatum	13.07.2023
Melder	Vladyslav Zubkov (schwytz)
Beschreibung	<p>Jede Anfrage an das E-Voting-System durchläuft einen Reverse-Proxy-Webserver. Dieser Reverse Proxy führt verschiedene Validierungen durch und enthält eine Web Application Firewall. Im Infrastruktur Whitepaper wird die Rolle des Reverse-Proxys erläutert. Gelegentlich führt der Reverse-Proxy eine HTTP-Umleitung durch. HTTP-Redirects sind eine Standardmethode, um einen Client, z. B. einen Webbrowser, darüber zu informieren, dass die angeforderte URL geändert wurde und stattdessen eine andere URL aufgerufen werden sollte. Es handelt sich um einen Mechanismus, der von Webservern eingesetzt wird, um den Browser eines Benutzers automatisch an einen anderen Ort umzuleiten.</p> <p>Wenn eine Anfrage einen bestimmten, nicht standardisierten HTTP-Request-Header enthält, leitet der Reverse-Proxy den Client zu einer Domäne um, die durch den "Host"-Wert der Anfrage angegeben wird. Der Reverse-Proxy sollte den Kunden nur zu einer Ressource mit derselben Domäne umleiten (z.B. pit.evoting.ch) und nicht zu einer anderen Domäne, die von einem Angreifer kontrolliert werden könnte. Aktuell validiert der Reverse-Proxy den "Host"-Wert im Request-Header nicht korrekt und akzeptiert Werte wie pit.evoting.ch.another.com. Es ist - allerdings nur theoretisch - möglich, einen Client auf eine falsche Webseite umzuleiten.</p> <p>Dies ist aber aufgrund der Sicherheitsvorkehrungen, dass eine HTTP-Anfrage nicht abgefangen werden kann, nicht möglich. Dennoch sollte der Reverse-Proxy das "Host"-Header-Feld korrekt validieren und nur erwartete Domänen akzeptieren, die in dieses Feld eingegeben werden.</p>
Status	<p>Der Melder weist darauf hin, dass es sehr unwahrscheinlich ist, dass diese Schwachstelle von einem Angreifer ausgenutzt werden kann, um ein realistisches Angriffsszenario zu erstellen. Das bedeutet, dass es einfach ist, die Schwachstelle selbst auszunutzen, aber praktisch ist es nicht möglich, einen Stimmberechtigten so fehlzuleiten.</p> <p>Dieser Bericht gilt als Verstoß gegen bewährte Praktiken, zeigt aber weder einen Angriffsvektor noch eine Schwachstelle auf. Dennoch wird die Konfiguration des Reverse-Proxys korrigiert, um dieses Verhalten zu verhindern.</p> <p>Die Post hat den Befund bestätigt und die Konfiguration im System korrigiert.</p>
Belohnung	Der Melder hat eine Belohnung von CHF 1000.- und zusätzlich einen Bonus von CHF 3000 erhalten.

4.2. Weitere nicht akzeptierte Befunde

Titel	Erkennen ungültiger Authentifizierungen beim Abfangen von Anfragen
Nummer	#YWH-PGM2323-185
Eingangsdatum	08.07.2023
Melder	No Breach
Beschreibung	Beim vorliegenden Befund hat der Melder Anfragen abgefangen und auf unterschiedliche Arten verändert. Obwohl er den korrekten Initialisierungscode und das für den Intrusionstest vorgegebene Geburtsjahr verwendete, antwortete der Wahlserver mit dem Status HTTP 401 Unauthorized auf die abgefangenen Anfragen. Im Befund weist der Melder darauf hin, dass es sich um ein Problem mit dem Authentifizierungsprotokoll handeln könnte.
Status	Als informativ geschlossen. Das Authentifizierungsprotokoll, das lose auf dem weit verbreiteten TOTP-Mechanismus (Time-based One-time Password) basiert, prüft die "Aktualität" einer Anfrage. Wenn eine Person die Anfrage für mehr als 30-60 Sekunden abfängt, ist die Authentifizierungsanfrage nicht mehr gültig und der Wahlserver lehnt die Authentifizierungsanfrage korrekt ab. Der beschriebene Mechanismus ist also so korrekt.
Belohnung	Keine

Titel	Angebliche Umgehung der Bestätigung der Stimme.
Nummer	#YWH-PGM2323-184
Eingangsdatum	08.07.2023
Melder	Xiety
Beschreibung	Der Melder vermutete, dass es möglich sei, die Bestätigung der Stimme zu umgehen, indem er einfach die Antwort einer erfolgreichen Bestätigung (die z. B. von einem anderen Stimmrechtsausweis stammen könnte) an dem Abstimmungsportal zurückschickt - obwohl der Wähler nicht den richtigen Bestätigungscode eingegeben hat.
Status	Als informativ geschlossen. Dieser Befund kann keine erkennbaren Auswirkungen auf die Sicherheit nachweisen, die über die Eigennutzung des eigenen Clients hinausgehen. Der festgestellte Mechanismus ist nur bei der Ausübung auf dem eigenen Computer möglich. Eine Manipulation einer dritten Person wäre nicht möglich und damit ist kein Risiko für die korrekte, sichere Stimmabgabe vorhanden. Eine stimmende Person kann auf keinen Fall – weder alleine noch mit Hilfe einer Drittperson – eine Stimme bestätigen, ohne dass sie ihren Bestätigungscode eingibt. Vom Server wurde der Versuch, eine Stimme mit einem ungültigen Bestätigungscode abzugeben, vom Evoting-System nicht berücksichtigt, wie aus der Serverantwort hervorgeht: " CONFIRMATION_KEY_INVALID". Daher bleibt die Stimme im unbestätigten Zustand und wird bei der Wahl nicht gezählt, so dass keine Sicherheitsauswirkungen erzielt wurden.
Belohnung	Keine

Titel	Angebliche Möglichkeit zur Abgabe mehrerer Stimmen.
Nummer	#YWH-PGM2323-186
Eingangsdatum	08.07.2023
Melder	Xiety
Beschreibung	Der Melder vermutete, dass es möglich ist, mehrere Stimmen für einen einzigen Stimmberechtigten abzugeben. Potenziell könnte ein Stimmberechtigter mehrere Stimmrechtsausweise herunterladen und sie zur mehrfachen Stimmabgabe für dieselbe Wahl verwenden. Für das Herunterladen von Wahlkarten gibt es keine Beschränkungen (z. B. aufgrund der IP-Adresse).
Status	Als informativ geschlossen. Die Musterstimmkarte auf https://www.evoting.ch/vc/ ist ausdrücklich zu Testzwecken vorgesehen. Während dem öffentlichen Intrusionstest können die Benutzer so viele Karten herunterladen, wie sie benötigen. Bei einer echten Wahl oder Abstimmung erhält jedoch jede und jeder Stimmberechtigte einen einzigen Stimmrechtsausweis mit den individuellen Codes per Post zugestellt
Belohnung	Keine

Die Einstufung der Befunde wird nach [Common Vulnerability Scoring System Version 3.1 Calculator \(first.org\)](https://www.first.org/cvss) vorgenommen.

4.3. 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 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) mit jeweils einer eigenen IP-Adresse angreifen konnten.

- Von rund 2650 unterschiedlichen IP-Adressen wurde im Laufe des öffentlichen Intrusionstest mittels der Protokolle HTTP/HTTPS auf den Server pit.evoting.ch zugegriffen.
- Von 42 IP-Adressen wurde versucht, über pit.evoting.ch Stimmen abzugeben.
- Von 32 IP-Adressen wurde mindestens eine Stimme erfolgreich abgegeben.
- Insgesamt wurden von 273 IP-Adressen jeweils mehr als 50 Zugriffe auf den E-Voting-Server gestellt. Diese werden als «aktivste Teilnehmende» bezeichnet.

4.3.1. IP-Adressen nach Ländern

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

Land	Anzahl IP-Adressen	Anteil
Deutschland	59	21.61%
USA	55	20.15%
Schweiz	27	9.89%
Frankreich	20	7.33%
Kanada	13	4.76%
Indien	12	4.40%
Tschechische Republik	7	2.56%
Litauen	5	1.83%
Portugal	5	1.83%
Singapur	5	1.83%
Finnland	4	1.47%
Tunesien	4	1.47%
Vietnam	4	1.47%
Belgien	3	1.10%
Rumänien	3	1.10%
Russland	3	1.10%
Türkei	3	1.10%
Grossbritannien	3	1.10%
Sonstige/Unbekannt	38	13.92%
Total	273	100.00%

4.4. Angriffe

4.4.1. Anzahl der Zugriffe

- Von den 2'650 IP-Adressen, die insgesamt Aktivität am öffentlichen Intrusionstest verzeichnet haben, gingen 471'141 Zugriffe aus.
- Im Durchschnitt gab es 178 Zugriffe, wobei der Median bei 3 Zugriffen pro IP-Adresse lag.
- Von den 273 IP-Adressen, die im öffentlichen Intrusionstest am meisten Aktivität verzeichnet haben, gingen insgesamt 446'661 Zugriffe auf der Domäne pit.evoting.ch aus, davon 89'708 auf dem E-Voting-Server aus, wovon über 53'000 als Angriffe einzustufen sind.

4.4.2. Statuscodes und Anzahl der Angriffe

Für die 446'661 Zugriffe sieht die Statistik mit den http-Statuscodes wie folgt aus:

Code	Code Message	Anzahl (auf pit.evoting.ch)	Anzahl (auf pit.evoting.ch/vote)	Anteil (auf pit.evoting.ch/vote)	Angriff
200	OK	26'511	10'587	11.80 %	-
302	Found	33'884	21'181	23.61 %	-
304	Not Modified	7'114	4'204	4.69 %	-
400	Bad Request	12'961	1'532	1.71 %	Ja
401	Unauthorized	5'023	0	0 %	Ja
403	Forbidden	359'745	52'052	58.02 %	Ja
404	Not Found	399	122	0.14 %	-
408	Request Timeout	233	28	0.03 %	-
500	Internal Server Error	694	0	0 %	Ja
405 406 413 415 417 429	Method Not Allowed Not Acceptable Content Too Large Unsupported Media Type Expectation Failed Too Many Requests	97	2	0 %	-
Gesamt		446'661	89'708	100%	-

Generelle Angriffe auf die E-Voting-Infrastruktur sind in Spalte 3 aufgeführt. In Spalte 4 sind gezieltere Angriffe auf den E-Voting-Server zu finden.

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.

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

4.4.3. Stimmabgabe

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

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

Prozessschritte	Anzahl Zugriffe	
Anmeldeversuche	12'304	von 74 unterschiedlichen IP-Adressen
Erfolgreiche Anmeldungen	239	von 49 unterschiedlichen IP-Adressen
Fehlgeschlagene Anmeldungen	12'065	von 25 unterschiedlichen IP-Adressen
Erfolgreiche Stimmabgaben	82	von 38 unterschiedlichen IP-Adressen
Fehlgeschlagene Stimmabgaben	19'645	von 12 unterschiedlichen IP-Adressen
Erfolgreich bestätigte Stimmen	59	von 32 unterschiedlichen IP-Adressen
Fehlgeschlagene Bestätigung der Stimme	16'112	von 10 unterschiedlichen IP-Adressen

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

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 13'390 Zugriffe aufgrund von Warnmeldungen blockiert, welche durch das CRS ausgelöst wurden. Einige der Warnmeldungen wurden ignoriert, da sie unter einer bestimmten Wertgrenze (Ungewöhnlichkeitsschwelle) lagen.

4.4.5. 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 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 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 177'262 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.

Statistiken:

- 5'039 Zugriffe durchliefen diese Prüfung erfolgreich.
- Bei 50 Zugriffen schlug diese Prüfung fehl und die Datei wurde nicht an den Abstimmungsclient gesandt. Die Analyse ergab, dass es sich dabei um Fehlalarme handelte, wo der Abstimmungsclient die Anfrage frühzeitig abgebrochen hat. Wir prüfen, wie wir in Zukunft diese Fehlalarme vermeiden können.
- Zu beachten ist, dass in Bezug auf diese möglichen Manipulationen keine Meldung eingegangen ist.

4.4.7. 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 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.

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
08.07.2023	24
09.07.2023	0
10.07.2023	0
11.07.2023	0
12.07.2023	0
13.07.2023	0
14.07.2023	33
15.07.2023	0
16.07.2023	0
17.07.2023	3
18.07.2023	66
19.07.2023	0
20.07.2023	0
21.07.2023	0
22.07.2023	0
23.07.2023	33
24.07.2023	0
25.07.2023	0
26.07.2023	0
27.07.2023	33
28.07.2023	33
29.07.2023	33
30.07.2023	0
31.07.2023	0

5. Zusammenfassung

Nachstehend findet sich eine Zusammenfassung zu den wichtigsten Ergebnissen aus dem öffentlichen Intrusionstest zum E-Voting-System der Post vom 08.07.-31.07.2023:

- **Teilnahme:** Es haben rund 2'650 IP-Adressen am öffentlichen Intrusionstest teilgenommen. Insgesamt hat die Post 273 IP-Adressen mit mehr als 50 Zugriffen von der gleichen IP-Adresse auf den E-Voting-Server verzeichnet. Mehr als 20 Prozent dieser «aktivsten Teilnehmenden» stammt aus Deutschland, rund 20 Prozent aus den USA und rund 10 Prozent aus der Schweiz. Im Vergleich zum letzten Jahr 2022 haben ca. 1000 IP-Adressen weniger teilgenommen, die Anzahl der «aktivsten Teilnehmenden» war jedoch ein Drittel höher.
- **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 verteilt. Bug Bounty Plattform, E-Voting-Blog, Mailings an Fachcommunity und institutionelle Stakeholder, Newsletter, Beiträge auf den Twitter- und LinkedIn Accounts der Schweizerischen Post und der Partnerin für das Bug-Bounty-Programm vor und während des PIT kommuniziert. Am 27.07.2023 wurde ein Interview mit dem ersten Melder eines bestätigten Befundes auf dem E-Voting-Blog gemacht, Weiter Beiträge auf den Twitter- und LinkedIn Accounts der Schweizerischen Post und der Partnerin für das Bug-Bounty-Programm zum Interview und zu den verbleibenden 5 Tagen des Intrusionstests wurden gemacht.
- **Angriffe:** Mit rund 2'650 unterschiedlichen IP-Adressen wurde im Zuge des öffentlichen Intrusionstest mittels der Protokolle HTTP/HTTPS insgesamt über 472'000 mal auf den E-Voting-Server zugegriffen, wobei mehr als 53'000 als Angriffe einzustufen sind.
- **Befunde:** Es ist keinem Hacker gelungen in das System einzudringen. Die Post hat vier Befunde erhalten, davon hat sie einen bestätigt. Es betrifft eine Verbesserung der Proxy-Konfiguration, welche als Best Practice gilt. Die Einstufung des Schweregrades ist «tief». Der Melder erhält für den Befund eine Belohnung von CHF 4'000.- und die Post setzt die Verbesserung um.

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 innerhalb des gesteckten Rahmens abwehren konnten.