Deutsche Lesefassung - Band 1

Schwachstellen elektronischer Wahl- und Auszählsysteme

CISA-Prüfbericht und NIC-Lagebewertung zur US-Wahlinfrastruktur

Grundlage: Vom Nutzer bereitgestellte, freigegebene Unterlagen der US-Regierung Stand der Übersetzung: 17. Juli 2026

Hinweise zu dieser Übersetzung

Diese Lesefassung übersetzt den lesbaren Inhalt der englischsprachigen Originaldokumente ins Deutsche. Wiederkehrende Freigabe-, Klassifizierungs-, Verteiler- und Kontaktvermerke werden zusammengefasst. Geschwärzte Stellen erscheinen als [GESCHWAERZT], technisch nicht sicher lesbare Stellen als [UNLESERLICH]. Erkennbare Fehler der maschinellen Texterkennung wurden anhand des sichtbaren Zusammenhangs berichtigt.

Die Neuformatierung ist keine amtliche Übersetzung. Die Aussagen werden in der Form wiedergegeben, in der sie in den Dokumenten stehen. Insbesondere wird zwischen einer technischen Fähigkeit, einer angenommenen Absicht, einem erkannten Zugriff und einer nachgewiesenen Veränderung von Stimmen oder Ergebnissen unterschieden.

Enthaltene Originaldokumente

1. `CISA Election Report - FINAL.pdf`, Stand 13. Juli 2026, 6 Seiten 2. `NICM_VulnerabilitiesInUS2020ElectionInfrastructure_15JAN2020_DECLASS_REDACTEDed.pdf`, 15. Januar 2020, 5 Seiten

---

1. CISA-Wahlbericht

Originaltitel: `Election Report` Originaldatei: `CISA Election Report - FINAL.pdf` Herausgeber: Cybersecurity and Infrastructure Security Agency (CISA) Stand: 13. Juli 2026 Originalumfang: 6 Seiten

Zusammenfassung

Von etwa 2019 bis 2024 führte CISA technische und operative Maßnahmen durch, um die Sicherheit bestimmter amerikanischer Wahlsysteme zu bewerten. Alle Maßnahmen erfolgten auf Bitte der jeweiligen Eigentümer oder Betreiber. Dazu gehörten die unmittelbare Untersuchung wahlbezogener Software, Penetrationstests in Netzen von Bundesstaaten, Kommunen, Stämmen und Territorien sowie Reaktionen auf Eindringversuche in Wahlsysteme.

Dadurch gewann CISA ein detailliertes Bild der Schwachstellen, die zum Zeitpunkt der jeweiligen Prüfung in ausgewählten Softwareprodukten und Netzwerkumgebungen bestanden. Wenn CISA eine Schwachstelle fand, informierte die Behörde den Eigentümer oder Betreiber und forderte zur Beseitigung auf.

Die Ergebnisse zeigen nach Darstellung des Berichts, dass wahlbezogene Software wie jede komplexe Software Schwachstellen enthält, die rechtzeitig behoben werden müssen. Frühere Partnerschaften mit Herstellern ermöglichten es, Sicherheitsprobleme bereits vor der Veröffentlichung eines Produkts zu erkennen. Strukturelle Vorgaben der Zertifizierung schränkten jedoch die Möglichkeit ein, Systeme schnell zu aktualisieren. Manche staatlichen Regelungen verlangten beispielsweise, dass in den Monaten vor einer Wahl keine Patches eingespielt werden. Zusammen mit uneinheitlichen Offenlegungspraktiken führe dies dazu, dass Wahlsysteme mit bekannten, nicht geschlossenen Sicherheitslücken eingesetzt würden.

Über die Softwarequalität hinaus zeigten die Prüfungen wiederholt Mängel der Cybersicherheit in den IT-Netzen lokaler und regionaler Wahlbehörden. Bedrohungsmodelle der Hersteller gingen oft von einer starken Trennung und Isolation der Wahlsysteme aus. In der Praxis sei Wahlinfrastruktur jedoch häufig aus allgemeinen Verwaltungsnetzen erreichbar. Wer ein E-Mail-System, einen Arbeitsplatzrechner oder andere IT-Komponenten kompromittiere, könne sich unter solchen Bedingungen seitlich im Netz in Richtung sensibler Wahlsysteme bewegen. Schwaches Identitätsmanagement, begrenzte Protokollierung und unzureichende Netztrennung erhöhten das Risiko eines Zugriffs oder einer Störung.

CISA nennt drei Faktoren, deren Zusammenspiel die Sicherheit amerikanischer Wahlen prägt:

- Das Management von Softwarelücken werde durch überholte Zertifizierungsregeln eingeschränkt.
- Hersteller informierten uneinheitlich über Schwachstellen und den Stand von Patches.
- Viele Netze der zuständigen Bundesstaaten, Kommunen, Stämme und Territorien hätten noch keine ausreichende Reife bei der Cybersicherheit.

Ziel und Untersuchungsmethoden

CISA stützte den Bericht auf Bewertungen aus dem Zeitraum 2019 bis 2025. Untersucht wurden nicht nur Wahl- und Registrierungsprogramme, sondern auch die größeren Verwaltungsumgebungen, in denen sie betrieben wurden, darunter E-Mail-Konten und sonstige Büro-IT.

Auf Bitte der jeweils zuständigen Stellen setzte CISA mehrere sich ergänzende Methoden ein:

- Analyse von Quellcode und ausführbaren Programmen;
- Prüfung von Protokollen und Schnittstellen;
- Penetrationstests und Red-Team-Einsätze gegen regionale und lokale Netze;

- Reaktion auf konkrete Cybersicherheitsvorfälle;
- Abgleich von Schwachstellen, Angreifertaktiken, Bedrohungsinformationen, Fehlkonfigurationen, Protokollierungslücken und Architekturproblemen.

Die Auswertung half laut Bericht, sogenannte Sicherheitsregressionen zu erkennen, bei denen eine Softwareänderung ein zuvor behobenes Problem erneut auftreten ließ. Erkannt wurden außerdem wiederkehrende wirkungslose oder schädliche Lösungsversuche sowie Bedingungen, unter denen Angreifer sensible Daten abziehen, wahlspezifische Dateien verändern oder die Verfügbarkeit von Systemen beeinträchtigen konnten.

Direkte Untersuchung von Wahlsoftware

Von 2019 bis 2024 arbeitete CISA mit dem Idaho National Laboratory im Programm `Critical Product Evaluation` zusammen. Auf freiwillige Bitte der jeweiligen Hersteller wurden Wahlsoftwareprodukte technisch untersucht, vielfach noch vor ihrer Veröffentlichung.

Die Prüfungen umfassten:

- automatisierte und manuelle statische Analyse des Quellcodes;
- Fuzzing von Parsern, Medienverarbeitung und Datenimportmodulen mit absichtlich unerwarteten Eingaben;
- Analyse der kryptografischen Umsetzung, etwa fehlerhafter Zufallszahlengeneratoren und unsicherer Schlüsselverwaltung;
- Tests von Authentifizierung, Berechtigungen und Grenzen von Programmierschnittstellen;
- Prüfung von Abhängigkeiten in der Lieferkette, darunter Fremdbibliotheken, Betriebssystempakete und gegebenenfalls Firmware;
- dynamische Analyse in gehärteten sowie absichtlich gegnerisch gestalteten Laufzeitumgebungen.

Die Hersteller betrachteten das Programm nach Darstellung von CISA im Allgemeinen als wertvoll. Das vertrauliche Modell habe jedoch zugleich Anreize gegen eine transparente Offenlegung nach branchenüblichen Standards geschaffen. Hersteller konnten Probleme vor der Markteinführung im Stillen beheben; nachgelagerte Betreiber, Risikoverantwortliche und externe Forscher erhielten aber keinen klaren Verlauf der gefundenen Schwachstellen oder der dazugehörigen Patches.

Das Programm wurde 2024 nach Rückmeldungen Beteiligter eingestellt; die abschließende Berichterstattung endete 2025.

Arten gefundener Schwachstellen

Nach der Auswertung von CISA enthielt Wahlsoftware das bei komplexen Systemen übliche Spektrum möglicher Fehler. Genannt werden:

- unzureichende Prüfung von Eingaben;
- unsichere Deserialisierung von Daten;
- unzureichende Ereignisprotokollierung;
- Race Conditions, die zu unvorhersehbaren Ergebnissen führen können;
- unsichere kryptografische Verfahren;
- Wege zur Ausweitung von Benutzerrechten.

Viele Schwachstellen seien von den Herstellern noch vor der Veröffentlichung schnell behoben worden. CISA habe jedoch nicht unabhängig überprüft, ob alle Korrekturen tatsächlich in den produktiven Fassungen enthalten waren, die bei regionalen und lokalen Wahlstellen eingesetzt wurden.

Hindernisse für Sicherheitsupdates

Regionale und lokale Wahlbehörden hätten Schwierigkeiten, Aktualisierungen rechtzeitig einzuspielen. Viele verfügten nur über geringe IT-Budgets und wenig Personal für Cybersicherheit. Einige Systeme würden nur im engen Zeitraum um eine Wahl betrieben. Andere liefen länger, würden aber in den Monaten oder Wochen vor dem Wahltag für Änderungen gesperrt. Teilweise seien solche Sperrfristen gesetzlich vorgeschrieben.

Gesetze einzelner Bundesstaaten könnten zusätzlich verlangen, ausschließlich Software einzusetzen, die von der Election Assistance Commission zertifiziert wurde. Erscheine eine Sicherheitsaktualisierung erst nach der Zertifizierung, könne sich ihr Einsatz weiter verzögern. Die unterschiedlichen Regeln schafften für die Hersteller eine zersplitterte Zertifizierungslandschaft.

Daraus leitet der Bericht folgende technische Risiken ab:

- Hersteller können Sicherheitskorrekturen oft nur in engen Zertifizierungsfenstern ausliefern, ohne die Zulassung für eine bevorstehende Wahl zu gefährden.
- Eingebaute Fremdkomponenten wie Betriebssysteme, Treiber, Middleware und Kryptobibliotheken können nicht im sonst üblichen Tempo aktualisiert werden.
- Veraltete Betriebssysteme und nicht mehr unterstützte Laufzeitkomponenten sammeln ungepatchte Schwachstellen an.
- Fehlende sichere automatische Aktualisierung verhindert eine schnelle Reaktion auf neu entdeckte Zero-Day-Lücken.

In der Praxis blieben bekannte und dokumentierte Schwachstellen dadurch nach CISA über Monate oder Jahre in produktiven Wahlsystemen bestehen. Die Zurückhaltung von Herstellern bei der öffentlichen Bekanntgabe von Lücken zertifizierter Produkte erschwere es Betreibern zusätzlich, Risiken informiert abzuwägen, Ersatzschutzmassnahmen zu prüfen oder ihre Netzarchitektur anzupassen.

CISA empfiehlt politischen Entscheidungsträgern deshalb, die Regeln für Patchmanagement und Zertifizierung zu vereinheitlichen. Wahlstellen sollten Sicherheitsupdates rechtzeitig einspielen können, während Hersteller nicht mit zahlreichen voneinander abweichenden Regelwerken umgehen müssen.

Sicherheitslage der Betriebsnetze

Wahlsoftware werde in Netze eingebaut, deren Schutz häufig nicht dem Reifegrad entspreche, den Hersteller in ihren Bedrohungsmodellen voraussetzten. In Penetrationstests und Red-Team-Einsätzen fand CISA wiederkehrende strukturelle Probleme:

- flache oder nur gering getrennte Netze, die Bewegungen aus normalen Verwaltungsbereichen wie E-Mail-Servern oder Fachanwendungen in Wahlumgebungen erlaubten;
- schwaches Identitäts- und Zugriffsmanagement, darunter unzureichende Mehrfaktor-Authentifizierung, gemeinsam verwendete Zugangsdaten und schlecht verwaltete Dienstkonten;
- fehlende Härtung von Endgeräten, veraltete Betriebssysteme, zu geringe Ereignisprotokollierung und unbeaufsichtigte Administrationsschnittstellen;
- alte Fernzugriffs- und Dateiübertragungswege, die weiterhin aus Netzbereichen erreichbar waren, von denen sie getrennt sein sollten;
- unzureichende Überwachung des Datenverkehrs, wodurch gegnerische Aktivitäten unentdeckt bleiben konnten.

In mehreren Fällen erlangten die CISA-Prüfer binnen Stunden oder Tagen die vollständige Kontrolle über ein Netz. Der Bericht folgert daraus, viele Partner seien leichte Ziele und könnten selbst Angreifer mit nur mittlerem technischen Können nicht aufhalten.

Papierwahl, ImageCast X und Puerto Rico

Die meisten Bundesstaaten seien von papierlosen elektronischen Wahlmaschinen abgerückt, weil diese keinen physischen Nachweis erzeugten und den Wählern keine Möglichkeit gäben, die korrekte Speicherung ihrer Auswahl zu kontrollieren.

Auch papiergestützte Ersatzsysteme könnten jedoch verwundbare Komponenten enthalten. CISA nennt als Beispiel `ImageCast X Ballot Marking Devices` aus dem Jahr 2020. Diese Geräte druckten ausgefüllte Stimmzettel auf Papier, kodierten die Auswahl aber zugleich in einem Strichcode, den der Wähler nicht selbst prüfen konnte. Ein Forscher habe gezeigt, dass Angreifer die im Strichcode gespeicherten Stimmen verändern könnten, ohne physischen Zugang zum Gerät zu haben.

Als Quelle nennt der Bericht die 2021 eingereichte Sicherheitsanalyse von J. Alex Halderman und Drew Springall im Verfahren `Curling v. Raffensperger`.

Das Office of the Director of National Intelligence ließ außerdem Dominion-Geräte untersuchen, die bei der Wahl 2024 in Puerto Rico verwendet worden waren. CISA habe den daraus entstandenen vorläufigen Bericht gelesen, aber keinen Zugang zu den Geräten gehabt und daher keine eigene technische Untersuchung durchführen können.

Scheitern angenommener Netztrennung

Bedrohungsmodelle der Hersteller setzten normalerweise eine strenge Trennung zwischen Wahlsystemen und der allgemeinen Verwaltungs-IT voraus. Zu den Wahlsystemen zählten Wählerregistrierungsdatenbanken, elektronische Wählerverzeichnisse, Wahlmanagement- und Auszählsysteme sowie zentrale Scanner.

Die CISA-Prüfungen von 2019 bis 2024 zeigten dagegen wiederholt:

- Wahlsysteme waren von Verwaltungsrechnern aus erreichbar, etwa wegen gemeinsam genutzter Authentifizierungsbereiche, alter VLAN-Konfigurationen oder als vorübergehend eingeführter Ausnahmen, die dauerhaft bestehen blieben.
- Firewallregeln erlaubten zu viel Verkehr; Kontrollen für ausgehende Verbindungen waren unzureichend.
- Wahlinfrastruktur lief auf allgemeinen Virtualisierungsclustern, die zugleich öffentlich erreichbare Dienste beherbergten.
- Betreiber verließen sich auf eine vermeintliche physische Netztrennung, die der realen Verbindungslage nicht entsprach. Als Beispiele nennt CISA Wartungstunnel der Hersteller, unbeaufsichtigte Fernverwaltungsprogramme und indirekte Netzwerkpfade.

Diese Abweichungen zwischen theoretischem Bedrohungsmodell und wirklicher Installation schufen ausnutzbare Wege: Ein Angreifer könne mit gewöhnlichem Phishing einen ersten Zugang erlangen und sich von dort zu besonders wertvollen Wahlkomponenten bewegen.

Bedeutung von Transparenz

Nach Auffassung von CISA haben amerikanische Bürger ein Recht zu erfahren, wenn Wahlinfrastruktur kompromittiert wurde und was bei einem Vorfall geschah. Hersteller und Kommunen könnten durch offene Anerkennung und die Beschreibung ihrer Gegenmassnahmen zeigen, dass sie kritische Infrastruktur aktiv schützen.

Klare und einheitliche Offenlegung stärke die Verantwortlichkeit der beteiligten Institutionen. Bereits der Eindruck von Geheimhaltung könne Vertrauen schneller untergraben als der Vorfall selbst. Eine frühe, regelmäßige und ehrliche Kommunikation solle zugleich sensible operative Einzelheiten schützen.

Empfohlene Gegenmassnahmen

CISA empfiehlt regionalen und lokalen Wahlbehörden:

1. Regeln für Patchmanagement und Zertifizierung von Wahlsystemen und zugehöriger IT so zu vereinheitlichen, dass Sicherheitskorrekturen in Echtzeit vorgenommen werden können, ohne die Zertifizierung zu verlieren; 2. die CISA-Empfehlungen zur Absicherung von Wahlsystemen einzuhalten; 3. für Menschen lesbare Papierstimmzettel zu verwenden; 4. nach der Wahl manuelle Prüfungen der Papierstimmzettel durchzuführen, um die beabsichtigte Funktion der Systeme zu bestätigen und Fehler vor der Ergebnisfeststellung zu erkennen; 5. Hersteller von Wahlsoftware dazu anzuhalten, - für ihre Schwachstellen CVE-Kennungen zu vergeben, - Kunden zu informieren, wenn Quellcode von Wahlsoftware abfließt oder gestohlen wird, - Cybersicherheitsvorfälle den zuständigen Stellen zu melden und - jedem Produkt eine Software-Stückliste, eine sogenannte SBOM, beizufügen; 6. alle Sicherheitsvorfälle und Behebungsprozesse klar, einheitlich und transparent zu dokumentieren.

Schlussfolgerung des Berichts

CISA sieht amerikanische Wahlsysteme denselben grundlegenden Sicherheitsproblemen ausgesetzt wie andere Softwaresysteme: veralteten und zersplitterten Zertifizierungsregeln, unzureichender Transparenz bei Schwachstellen und dauerhaften Sicherheitslücken in den Betriebsnetzen.

Diese Probleme seien nicht einer einzelnen Stelle zuzuschreiben, sondern entstünden aus komplexen Abhängigkeiten zwischen Herstellern, Zertifizierern, politischen Entscheidungsträgern und finanziell oder personell eingeschränkten Wahlbehörden.

Notwendig seien nachhaltige Investitionen in Netzmodernisierung, Segmentierung, Identitätsmanagement und Überwachung. Papiernachweise, gründliche manuelle Nachwahlprüfungen, Software-Stücklisten und eine bessere Erfassung von Vorfällen ermöglichten nach Darstellung von CISA messbare Verbesserungen in absehbarer Zeit.

2. Schwachstellen der US-Wahlinfrastruktur 2020

Originaltitel: `Vulnerabilities in US 2020 Election Infrastructure` Originaldatei: `NICM_VulnerabilitiesInUS2020ElectionInfrastructure_15JAN2020_DECLASS_REDACTEDed.pdf` Herausgeber: National Intelligence Council Dokumentkennung: NICM 2020-003 Datum: 15. Januar 2020 Freigabe: Am 16. März 2026 durch die Direktorin der nationalen Nachrichtendienste Tulsi Gabbard freigegeben; am 3. Juli 2026 von Präsident Trump zur Veröffentlichung genehmigt Originalumfang: 5 Seiten

Umfang und Kernaussage

Das Memorandum bewertet die möglichen Auswirkungen von Cyberoperationen gegen die amerikanische Wahlinfrastruktur bei der Präsidentschaftswahl 2020. Es behandelt den Wahlvorgang und die Integrität der Ergebnisse. Die Absichten ausländischer Akteure und deren eigene Sicht auf amerikanische Schwachstellen sind ausdrücklich nicht Gegenstand des Papiers.

Das National Intelligence Council bewertet, dass mindestens Russland, China, Iran und Nordkorea technisch in der Lage seien, auf Daten in wahlbezogenen amerikanischen Computersystemen zuzugreifen und sie möglicherweise zu verändern. Ob diese Staaten konkrete Pläne hatten, die Funktion solcher Systeme zu stören, sei unbekannt.

Die Kernaussagen lauten:

- Zentralisierte wahlbezogene Datenspeicher wie Wählerregistrierungsdatenbanken, Wählerverzeichnisse und offizielle Wahlwebseiten seien am leichtesten auszunutzen. Ein Zugriff könne Wahlabläufe stören.
- Systeme zur Auszählung, Übertragung oder Anzeige von Ergebnissen seien lokal angreifbar. Eine Veränderung in einem Umfang, der das Gesamtergebnis einer Präsidentschaftswahl beeinflusse, sei jedoch schwierig.
- Falsche Behauptungen eines Gegners, er habe Systeme oder Ergebnisse manipuliert, wären schwer zu widerlegen und könnten das Vertrauen in die Wahl untergraben.
- Die genannten Staaten und auch nichtstaatliche Gruppen hätten die Fähigkeit, Wahlinfrastruktur zu kompromittieren. Ein solcher Zugriff könne Abläufe stören, sensible Daten entwenden oder Zweifel an Ergebnissen säen. Konkrete Pläne zur Manipulation seien dem Papier jedoch nicht bekannt.

Russland habe im Wahlzyklus 2016 fast sicher die Wahlnetze sämtlicher Bundesstaaten ausgekundschaftet, in mindestens zwei Staaten Zugriff auf wahlbezogene Infrastruktur erlangt und aus mindestens einem Staat Wählerdaten abgezogen. Aufgrund bekannter Fähigkeiten und früherer Operationen seien Russland, China, Iran und Nordkorea zu ähnlichen Aktivitäten im Wahlzyklus 2020 fähig gewesen.

Fortgeschrittene Einbruchs- und Angriffswerkzeuge seien zudem im Darknet erhältlich. Dadurch könnten weitere Staaten und nichtstaatliche Akteure in die Lage versetzt werden, eine Wahl zu stören. Auch Cyberkriminelle und Hacktivisten könnten aus finanziellen oder politischen Motiven Wahlinfrastruktur angreifen.

Begriffsbestimmungen des Dokuments

Angriff: Ein Cyberakteur versucht, den Betrieb eines Systems oder Netzes zu beeinträchtigen, zu zerstören, zu stören, zu manipulieren oder anderweitig zu behindern. Die Veränderung oder Löschung von Daten allein zur Verschleierung eines Eindringens gilt nicht als Angriff.

Kompromittierung: Ein Cyberakteur erlangt unbefugten Zugang, um Daten zu sammeln oder Befehle auszuführen, oder installiert Schadsoftware, die mit einer bösartigen IP-Adresse verbunden ist.

Ausnutzung: Ein bösartiger Akteur sammelt Daten, installiert weitere Schadsoftware oder richtet einen dauerhaften Zugang zu einem kompromittierten System ein. Akteure können mehr Konten und Systeme kompromittieren, als sie anschließend tatsächlich ausnutzen, unter anderem weil automatisierte Werkzeuge in großem Umfang verwundbare Systeme finden.

Scan: Ein Akteur sendet einem System gezielten Netzwerkverkehr und wertet dessen Antworten aus, um Sicherheitslücken festzustellen. Internetscans seien sehr verbreitet, hätten aber oft nur eine geringe Erfolgsquote; deshalb würden weit mehr Systeme gescannt als tatsächlich betroffen.

Zentralisierte Datenspeicher

Nach der Bewertung ließen sich zentralisierte wahlbezogene Datenbestände wegen ihrer einfachen Erreichbarkeit und vergleichsweise geringen Absicherung am leichtesten ausnutzen. Die Systeme sammelten, aktualisierten und speicherten Wählerinformationen. Sie seien für regelmäßigen Zugang, häufig über Webportale, ausgelegt und dadurch für unterschiedliche bösartige Cyberaktivitäten offen.

Ein entschlossener Gegner könne einen solchen Zugang nutzen, um Wahlabläufe landesweit zu stören.

Wählerregistrierungsdatenbanken

Die meisten Staaten betrieben ihre Registrierungsdatenbanken auf mit dem Internet verbundenen Systemen. Der Zugang sei absichtlich einfach gestaltet, weil die Daten nahezu fortlaufend aktuell gehalten werden müssten.

Ein Gegner könne Daten verändern, um einzelne Wähler oder Gruppen möglicherweise an der Stimmabgabe zu hindern, am Wahltag Verzögerungen zu erzeugen oder Betroffene zur Abgabe provisorischer Stimmzettel zu zwingen. Registrierungsdaten, die teilweise auch öffentlich oder käuflich seien, könnten außerdem für andere Einmischungs- oder Einflussaktivitäten zugeschnitten werden.

Elektronische und gedruckte Wählerverzeichnisse

Registrierungsdatenbanken übermittelten Angaben an elektronische oder papiergebundene Verzeichnisse, mit denen Wähler im Wahllokal eingecheckt würden. Manche elektronischen Verzeichnisse seien mit internetverbundenen Datenbanken gekoppelt. Ein Gegner könne diese nach Bewertung des Papiers wahrscheinlich leicht ausnutzen und Daten mit ähnlichen Folgen wie bei einem Angriff auf die Registrierungsdatenbank verändern.

Webseiten von Wahlbehörden

Staatliche und lokale Webseiten informierten über Wahllokale und dienten in einigen Staaten zur Veröffentlichung von Ergebnissen. Angriffe oder Kompromittierungen könnten Menschen von der Stimmabgabe abhalten oder Zweifel an den Ergebnissen hervorrufen.

Systeme zur Durchführung und Auszählung der Wahl

Systeme, die Stimmen auszählen, Summen übermitteln oder Ergebnisse anzeigen, seien wahrscheinlich lokal ausnutzbar. Eine Manipulation in großem Maßstab sei jedoch schwer. Das Dokument verweist darauf, dass Sicherheitsforscher mehrfach gezeigt hätten, wie leicht sich bestimmte Wahlmaschinen kompromittieren ließen.

Direktaufzeichnende elektronische Wahlmaschinen speicherten Stimmen und Auszähldaten digital, teilweise auf austauschbaren Speichermedien. Besonders anfällig seien Modelle ohne

Papiernachweis. Solche Maschinen würden allerdings deutlich seltener eingesetzt als sicherere Varianten.

Wer physischen Zugang zu einer Wahlmaschine erlange, könne nach staatlichen und akademischen Untersuchungen ihre Funktion verändern, Daten manipulieren oder Schadsoftware installieren. Auf der Sicherheitskonferenz DEF CON 2019 demonstrierten Teilnehmer die Kompromittierung von mehr als 100 Wahlmaschinen. Jede dieser Maschinen war nach dem Dokument für die Nutzung in mindestens einem amerikanischen Wahlbezirk zertifiziert.

Als anschauliches Beispiel nennt das Papier ein elektronisches Wählerverzeichnis, das im `Voting Machine Hacking Village` der DEF CON 2019 so verändert wurde, dass darauf das Computerspiel `Doom` lief.

Elektronische Rücksendung von Briefwahlstimmen

Einunddreissig Bundesstaaten und der District of Columbia erlaubten berechtigten Wählern, Briefwahlstimmen per Internet oder Fax einzureichen. Dadurch seien diese Stimmen für Störung oder Manipulation anfällig.

Vier Staaten erlaubten die Rücksendung über ein Webportal, sieben bestimmten Wählern ausschließlich per Fax und ein Staat über eine mit Blockchain-Technik abgesicherte mobile Anwendung. Die Zahl solcher Stimmen sei jedoch gering; zudem würden sie normalerweise besonders aufmerksam auf Auffälligkeiten kontrolliert.

Vorbereitung von Stimmzetteln und Wahlmaschinen

Die Vorbereitung von Papier- und elektronischen Stimmzetteln sowie von Maschinen sei gegenüber Cyberangriffen, Lieferkettenangriffen und Innentätern verwundbar. Nach Bewertung des Dokuments machten die vorhandenen Schutzmassnahmen und die landesweit verteilten Lager- und Vorbereitungsorte eine koordinierte Manipulation eines ganzen Bundesstaats oder mehrerer Staaten jedoch schwierig.

Die Erstellung von Stimmzetteln oder Dateien für Wahlmaschinen werde häufig an Drittanbieter vergeben. Einige nutzten internetverbundene Computersysteme und hätten keine ausreichenden Regeln für Passwörter oder Verschlüsselung. Ein Angreifer könne deshalb Stimmzetteldateien beschädigen. Logik- und Genauigkeitstests vor dem Wahltag würden eine solche Veränderung wahrscheinlich erkennen.

Würden Wahlmaschinen an einem zentralen Ort eingerichtet, entstehe ein Risiko durch Innentäter. In dieser Phase eingebrachte Schadsoftware könne mehrere Wahlbezirke betreffen, wäre aber ebenfalls bei den Tests vor der Wahl erkennbar.

Begrenzung großflächiger Manipulation

Das Memorandum bewertet, dass sich Auszählsysteme nur schwer in einem Umfang manipulieren ließen, der das Wahlergebnis insgesamt beeinträchtigte. Die Systeme der einzelnen Wahllokale seien nicht miteinander oder mit dem Internet verbunden. Viele Angriffsmethoden setzten räumliche Nähe voraus.

Ein Gegner könne theoretisch mehrere Wahlbezirke und genügend Bundesstaaten beeinflussen, um auf eine Präsidentschaftswahl einzuwirken. Eine solche Kampagne sei jedoch schwierig; Nachwahlprüfungen und Papiernachweise würden sie sehr wahrscheinlich aufdecken.

Eine wachsende Zahl von Wahlbezirken nutze vom Wähler kontrollierbare Papiernachweise und Nachwahlprüfungen. Solche Prüfungen seien damals in 38 Staaten vorgeschrieben und könnten Wahlverantwortliche auf Manipulation oder Fehler hinweisen.

Cyberoperationen gegen die elektronische Auszählung könnten die Ergebnisveröffentlichung betroffener Bezirke verzögern und dadurch Unsicherheit erzeugen. Die Integrität der später amtlich festgestellten Ergebnisse werde davon wahrscheinlich nicht berührt.

Ausgezahlte Ergebnisse würden getrennt von den Kopien gespeichert, die auf Ergebniswebseiten angezeigt werden. Ermittlungen nach einem Angriff könnten gleichwohl die Bekanntgabe verzögern und Zweifel an der Gültigkeit der Zahlen hervorrufen. Überlastungsangriffe oder eine Veränderung der auf dem Übertragungsweg befindlichen Anzeigekopien könnten den öffentlichen Zugang verzögern oder den Eindruck veränderter Ergebnisse erwecken.

Eine Kommission zu Schwachstellen der Wahlinfrastruktur Pennsylvanias hatte festgestellt, dass die Übertragung vorläufiger Ergebnisse an öffentliche Webseiten für `Man-in-the-Middle`-Angriffe anfällig sei. Dabei verändere ein Angreifer Daten während der Übertragung. Die getrennt und offline verarbeiteten amtlichen Auszählungskopien würden dadurch nicht verändert; schon kurze Verzögerungen könnten jedoch Zweifel an Sicherheit oder Gültigkeit wecken.

Im Mai 2019 machten unbekannte Cyberakteure die Wahlwebseite eines amerikanischen Countys in der Nacht einer Bürgermeistervorwahl unerreichbar. Die Auszählung war nicht betroffen, weil sie auf einem getrennten, nicht mit dem Internet verbundenen System gespeichert wurde.

Falsche Manipulationsbehauptungen

Gegner könnten auch wahrheitswidrig behaupten, sie hätten amerikanische Wahlinfrastruktur manipuliert. Ein großer Teil der Öffentlichkeit kenne die technischen und organisatorischen Einzelheiten einer Wahl vermutlich nicht, wodurch falsche Erzählungen leichter Fuß fassen könnten.

Staatliche Untersuchungen und eine öffentliche Widerlegung könnten Wochen oder Monate dauern. In dieser Zeit könnten Zweifel wachsen. Eine Behauptung wäre unter Umständen gar nicht widerlegbar, wenn der Gegner der amerikanischen Nachrichtengewinnung entgangen sei.

Das Dokument nennt drei Varianten:

- Ein Gegner könne vollständig erfundene Behauptungen aufstellen, etwa alle amerikanischen Wahlmaschinen kompromittiert zu haben. Das wäre zeitaufwendig oder unmöglich zu widerlegen.
- Er könne eine übertriebene Behauptung über die Beeinflussung des Wahlausgangs mit einem tatsächlichen, aber begrenzten Vorgang verbinden, etwa einem Überlastungsangriff auf Wahlwebseiten oder einem Eindringen in Registrierungsdatenbanken. Obwohl dies nicht die Abgabe, Auszählung oder amtliche Meldung von Stimmen betreffe, könne die Verbindung Zweifel am ganzen Ergebnis auslösen.
- Bereits eine stark beachtete Kompromittierung könne das Vertrauen untergraben, selbst wenn keinerlei wahlbezogene Daten oder Systeme verändert wurden.

Vorgeschlagene Schutzmassnahmen

Das Papier bewertet, dass verbesserte physische Sicherheit, stärkere Cyberschutzmassnahmen und gezielte Kommunikation mit der amerikanischen Öffentlichkeit und möglichen Gegnern einen Teil der Risiken mindern könnten.

Physische Sicherheit und Cyberhygiene: Veraltete Geräte ersetzen, Passwortregeln und Prüfverfahren stärken sowie Netze segmentieren. Solche Grundlagen könnten weniger anspruchsvolle Angreifer abhalten, reichten aber wahrscheinlich nicht gegen die fortgeschrittensten und entschlossensten staatlichen Akteure.

Prüfung von Drittanbietern: Verbesserte Kontrollen von Herstellern und Zwischenhändlern der Wahlinfrastruktur könnten gemeinsame Schwachstellen oder Innentäter-Risiken sichtbar machen.

Öffentliche Information: Schnelle und genaue Mitteilungen sollten Wirkung und begrenzten Umfang kleinerer Cybervorfälle erklären. Partnerschaften mit staatlichen und lokalen Wahlstellen,

Sicherheitsunternehmen und Medien könnten Störungen begrenzen und cybergestützten Informationsoperationen entgegenwirken. Informationen bereits vor der Wahl sollten die Ziele von Gegnern erklären und amerikanische Behörden als verlässliche Quelle zu Integrität, Wiederherstellung und Ermittlungen etablieren.

Botschaften an Gegner: Vertrauliche Mitteilungen sollten verdeutlichen, dass Versuche zur Manipulation amerikanischer Wahlinfrastruktur nicht hinnehmbar seien und ernste Folgen hätten. Dies könne abschreckend wirken.

Einordnung des Aussageumfangs

Das Memorandum beschreibt technische Verwundbarkeit und mögliche Folgen. Es sagt zugleich ausdrücklich, dass zum damaligen Zeitpunkt keine konkreten Pläne der genannten Staaten zur Manipulation wahlbezogener Systeme bekannt waren. Für eine großflächige Veränderung eines Präsidentschaftswahlergebnisses nennt es erhebliche praktische Hindernisse und verweist auf Papiernachweise, Vorwahltests und Nachwahlprüfungen als mögliche Entdeckungsmechanismen.

Dokumentenstatus und Übersetzungsvermerk

Der CISA-Bericht beschreibt Ergebnisse technischer Prüfungen aus den Jahren 2019 bis 2025. Das NIC-Memorandum von Januar 2020 ist eine vorausschauende Fähigkeits- und Risikobewertung. Beide Dokumente behandeln Schwachstellen und Angriffspfade; daraus folgt allein kein Nachweis, dass eine bestimmte Schwachstelle in einer konkreten Wahl ausgenutzt oder ein amtliches Ergebnis verändert wurde.

Ende von Band 1