epochtimes.de

Cyber-Koryphäe Dr. Keshavarz-Nia: „Manipulation im großen Stil“ – „Beweise überwältigend und unbestreitbar“

Youtube-Kanal Frontal+

17-20 Minuten

Der prominente Cybersicherheits- und Geheimdienstexperte sagt in einer eidesstattlichen Erklärung, dass die Ergebnisse der Präsidentschaftswahl in den Swing States gefälscht und zugunsten Biden manipuliert wurden.

Dieser Artikel ist der Text zum Video: „Beweise überwältigend und unbestreitbar“: Geheimdienstexperte über Dominion Systems und die US-Wahl vom Youtube-Kanal „FRONTAL+“.

Im Machtpoker um die Präsidentschaftswahl in Amerika bekam die Anwältin Sidney Powell schwergewichtige Unterstützung. Der prominente Cybersicherheits- und Geheimdienstexperte Dr. Navid Keshavarz-Nia untermauerte Powells Anschuldigungen einer groß angelegten Manipulation der Präsidentschaftswahl im November zugunsten des Demokraten Joe Biden.

Dr. Keshavarz-Nia sagte in einer eidesstattlichen Erklärung, dass die Ergebnisse der Präsidentschaftswahl in den Swing States – also den für den Wahlausgang entscheidenden US-Bundesstaaten – gefälscht und Hunderttausende Stimmen für US-Präsident Donald Trump auf seinen Rivalen Joe Biden

übertragen worden seien.

Das sind schwerwiegende Anschuldigungen. Weil Dr. Navid Keshavarz-Nia möglicherweise eine Schlüsselrolle in den kommenden Gerichtsverfahren um die vermeintlichen Wahlfälschungen spielen wird, möchten wir die heutige Ausgabe von „Frontal Plus“ nutzen, um die wesentlichen Punkte seiner Erkenntnisse zusammenzufassen. Es wird unvermeidlich ein wenig technischer werden, aber bleiben Sie dran, wir werden es auch für interessierte Laien – so wie mich – verständlich halten.

Wer ist dieser Dr. Keshavarz-Nia eigentlich?

Der Ingenieur Dr. Keshavarz-Nia ist kein Unbekannter. Ganz im Gegenteil: Er ist bei Fachleuten seines Metiers hoch angesehen. Aktuell arbeitet Dr. Keshavarz-Nia für einen großen Auftragnehmer des Verteidigungsministeriums als Chefingenieur für die Sicherheit und als Sachverständiger für Cybersicherheit. In seiner jahrzehntelangen Karriere war er vielfach für Geheimdienste tätig.

In seiner Erklärung sagte der 59-Jährige:

> Im Laufe meiner Karriere habe ich Sicherheitsbeurteilungen, Datenanalysen und Sicherheitsabwehr sowie forensische Untersuchungen an Hunderten Systemen durchgeführt. Ich verfüge über 35 Jahre Erfahrung in den Bereichen technische Bewertung, mathematische Modellierung, Analyse von Cyber-Angriffsmustern und Sicherheitsabwehr in Verbindung mit China, Iran, Nordkorea und Russland.
>
> Ich habe als Berater und Fachexperte zur Unterstützung des Verteidigungsministeriums, des FBI und der US-Geheimdienste wie DIA, CIA, NSA, NGA und des DHS gearbeitet, um die

> Spionageabwehr zu unterstützen, einschließlich der Unterstützung von Ermittlungen der Strafverfolgungsbehörden.“

Dr. Keshavarz-Nia, der derzeit in Kalifornien lebt, genießt einen ausserordentlich guten Ruf. Noch vor wenigen Monaten lobte die „New York Times“ den Ingenieur in den höchsten Tönen, weil er eine entscheidende Rolle bei der Aufdeckung eines Betrügers namens Garrison Courtney spielte, der sich als CIA-Agent getarnt hatte. Diejenigen, die mit Keshavarz-Nia zusammenarbeiteten, sagten: „Er war immer die klügste Person im Raum.“ Das schrieb die „New York Times“ am 9. September 2020 in ihrem Bericht mit dem Titel „How One Man Conned the Beltway“.

Das US-Magazin „Washington Monthly“ äußerte sich ähnlich positiv über Dr. Keshavarz-Nia. In einem Artikel vom 17. September mit dem Titel „The Spy Was a Grifter“, (zu Deutsch: „Der Spion war ein Betrüger“) wurde der Experte als „Held“ bezeichnet, weil er Courtney entlarvt hatte. Garrison Courtney wurde im Oktober dieses Jahres wegen eines ausgeklügelten Betrugs, der ihm mindestens 4,4 Millionen US-Dollar einbrachte, zu sieben Jahren Haft verurteilt.

Analyse der Wahldaten von „New York Times“

Da die Aussagen von Dr. Keshavarz-Nia in Bezug auf die US-Wahl sehr brisant sind, kann es durchaus passieren, dass er öffentlich diskreditiert und seine Glaubwürdigkeit in Zweifel gezogen wird.

Dem Cyberexperten wurde es nicht erlaubt, eines der bei der Wahl 2020 verwendeten Systeme von Dominion zu untersuchen. Stattdessen führte er eine detaillierte Analyse der Wahldaten durch, die die „New York Times“ veröffentlichte. Er

kam zum dem Ergebnis, dass die Verteilung der Stimmenzahl in Pennsylvania, Wisconsin, Michigan, Arizona, Nevada und Georgia durch eine betrügerische elektronische Manipulation verursacht worden sein muss, die gezielt auf die Wahlautomaten ausgerichtet war.

Sehen wir uns nun im Detail an, wie der Wissenschaftler zu diesem Ergebnis gekommen war.

„Man-in-the-Middle“-Angriff beim Wahlsystem Dominion

Dr. Keshavarz-Nia erklärte, dass eine weit verbreitete Sicherheitslücke in den Wahlsystemen und der Software von Dominion einen sogenannten „Man-in-the-Middle“-Angriff durch unsichtbare Hintermänner ermögliche. Ein „Man-in-the-Middle“-Angriff ist eine Angriffsform, die in Rechnernetzen Anwendung findet. Der Angreifer steht dabei zwischen zwei Kommunikationspartnern und hat mit seinem System die vollständige Kontrolle über den Datenverkehr zwischen zwei oder mehreren Netzwerkteilnehmern und kann so die Informationen nach Belieben einsehen und sogar manipulieren – wie ein Januskopf (ein Kopf mit einem Gesicht vorne und einem hinten). Die Janusköpfigkeit des Angreifers besteht darin, dass er den Kommunikationspartnern vortäuscht, das jeweilige Gegenüber zu sein.

Der Sicherheitsexperte erklärte weiter:

> Der „Man-in-the-Middle“-Angriff erfolgte auf zwei Arten: Zunächst benutzten Mitarbeiter vor Ort USB-Speicherkarten, die kryptografische Schlüssel enthielten, die durch Hintertüren einen Zugang zum System ermöglichten, um dann die Abstimmungsresultate in den umkämpften Staaten zu

> verändern.
>
> Anschließend wurden diese Ergebnisse über Barcelona in Spanien an die Server von Scytl mit Sitz in Frankfurt am Main, Deutschland, weitergeleitet. Durch den „Man-in-the-Middle“-Angriff wurde sichergestellt, dass ausreichende Datenänderungen vorgenommen werden konnten, bevor die ausgewerteten Ergebnisse an das System von Scytl weitergeleitet wurden. Um den „Man-In-The-Middle“ zu verschleiern und eine Überwachung durch die US-Geheimdienste zu vermeiden, wurden die Wahldaten über das Ausland geleitet.“

Später werden wir noch einmal auf diese Server zu sprechen kommen, aber hören wir zunächst, was der Cyberexperte über die „Man-in-the-Middle“-Angriffe zu sagen hat.

Hammer- und Scorecard-Instrumente wurden von US-Geheimdiensten entwickelt

Der „Man-in-the-Middle“-Angriff sei mittels Hammer- und Scorecard-Instrumenten durchgeführt worden. Diese Instrumente seien, so Dr. Keshavarz-Nia, von den US-Geheimdiensten entwickelt worden. Dies wurde auch von der Enthüllungsplattform „WikiLeaks“ berichtet und später vom Drei-Sterne-Generalleutnant Thomas McInerney bestätigt, einem Veteran der United States Air Force, sowie von Kirk Wiebe, einem ehemaligen NSA-Beamten, und von Dennis Montgomery, einem ehemaligen CIA-Analysten.

Demnach handelt es sich bei den Hammer- und Scorecard-Instrumenten um Spionagetechniken, die von Agenten des US-Geheimdienstes verwendet werden, um „Man-in-the-Middle“-Angriffe auf ausländische Wahlsysteme, einschließlich

des Dominion Voting Systems, durchzuführen, ohne Spuren zu hinterlassen.

Smartmatics Software-Algorithmus hat die Stimmenauszählung manipuliert

Dr. Keshavarz-Nia sagte:

> Nach der Analyse der Wahldaten der „New York Times“ im Jahr 2020 kam ich zu dem Schluss, dass ein Software-Algorithmus die Stimmenauszählung manipuliert hat, um die Wahlergebnisse in den Bezirken der betroffenen Staaten zwischen 1% und 2% zugunsten von Joe Biden zu fälschen. Die Software führte die Datenänderung in Echtzeit durch, um eine enge Parität unter den Kandidaten aufrechtzuerhalten, ohne einen Verdacht zu erwecken. Der spezifische Software-Algorithmus wurde von Smartmatic entwickelt und in die Dominion-Maschinen implementiert, um einem betrügerischen Operator den Backdoor-Zugriff zur gewünschten Manipulation von Live-Daten zu erleichtern.“

Hintertüren im Dominon-System bereits früher entdeckt

Dr. Keshavarz-Nia führte im Laufe seiner Karriere forensische Analysen von elektronischen Wahlsystemen durch, darunter auch die Systeme von Dominion, wie das Democracy Suite Election Management System (EMS) und Election Systems & Software. Zudem analysierte er die SOE Software von Scytl und die Smartmatic-Systeme, die in Hunderten Bezirken in den wichtigsten Bundesstaaten bei dieser Wahl im Einsatz waren.

Dr. Keshavarz-Nia hat bereits früher größere Schwachstellen in den Dominon-Systemen entdeckt, wodurch ein Zugriff auf

sensible Funktionen möglich war. Durch eingebaute Hintertüren (auch Backdoors genannt) könnten, erklärt der Experte, Befehle von unbekannten Personen durchgeführt werden. Diese Hintertüren ermöglichten es einer Person, über das Internet Zugang auf das System zu erhalten, ohne entdeckt zu werden. Weiter sagte er:

> Diese Hintertüren könnten jedoch auch dazu verwendet werden, illegale Aktivitäten wie das Verschieben, Löschen oder Hinzufügen von Stimmen in Echtzeit durchzuführen. Diese Modifikationen können über das Internet und ohne eine Spur zu hinterlassen durchgeführt werden.“

„Manuelle Eingabe von mehr als 400.000 Stimmen innerhalb von 2-3 Stunden unmöglich“

Dr. Keshavarz-Nia konnte seinen Studien der Netzwerkkommunikation entnehmen, dass die Daten des Dominion Systems an IP-Adressen übertragen werden, die bei Scytl im spanischen Barcelona registriert sind, und dass Scytl seine Server in einem Rechenzentrum in Barcelona zum Zweck der Datensicherung unterhielt. Im Jahr 2020 wurde dieses Rechenzentrum dann nach Frankfurt am Main verlegt. Dr. Keshavarz-Nia ging davon aus, dass die Wahldaten aus der Präsidentschaftswahl in diesem Jahr auch dorthin übertragen wurden. Auf die Berichte über die Beschlagnahmung dieser Server in Frankfurt sind wir bereits in früheren Folgen eingegangen.

Nach Einschätzung des Experten hätten die Democracy Suite von Dominion, die Scytl-Software und Smartmatic bei der Wahl 2020 keine überprüfbaren Ergebnisse generiert. Er sagte:

> Es ist offensichtlich, dass die Stimmzettel nicht ordnungsgemäß

> validiert wurden, dass keine Systemaufzeichnungen gemacht wurden und dass das System selbst einige Tage vor dem 4. November 2020 eine erhebliche Instabilität aufwies, sodass Dominion in letzter Minute Softwareänderungen vornehmen musste. Darüber hinaus zeigt eine ungleiche Datenverteilung am Morgen des 4. November nach 4:30 Uhr erhebliche systematische Anomalien, die in allen Swing States auftraten. Die Beweise sind umfassend und überzeugend und deuten auf einen groß angelegten Betrug durch Hintermänner hin.“

Weiter sagte er, dass sich die Datenabweichung zugunsten von Joe Biden nach 4:30 Uhr am morgen des 4. November weiter beschleunigt und bis zum 9. November angehalten habe. Es habe am 4. November einen ungewöhnlich steilen Anstieg der Stimmen für Biden in allen Bundesstaaten gegeben. Ein so plötzlicher Anstieg sei nicht normal und zeige:

> … dass Daten mit künstlichen Mitteln manipuliert wurden. Zum Beispiel wurde in Pennsylvania der Vorsprung von Präsident Trump von mehr als 700.000 Stimmen in wenigen Stunden auf weniger als 300.000 reduziert, was in der realen Welt ohne äußeren Einfluss nicht vorkommt.“

Zudem kam er zu dem Schluss, „dass die manuelle Eingabe von mehr als 400.000 Stimmen aus Briefwahlscheinen in einem so kurzen Zeitrahmen, also innerhalb von zwei bis drei Stunden, ohne eine illegale Modifizierung unmöglich ist“.

Dominions Verbindung zu Venezuela

Die Dominion Voting Systems Corporation wurde 2003 in Toronto, Kanada, von John Poulos und James Hoover gegründet. Das Unternehmen entwickelt patentgeschützte Software und verkauft Hardware und Software für die

elektronische Stimmabgabe, einschließlich Wahlgeräte und Tabulatoren, in den Vereinigten Staaten und anderen Teilen der Welt. Laut Dr. Keshavarz-Nia soll Dominion eine strategische Beziehung zu Venezuelas Bitza Corporation unterhalten haben, die sich zu 28 Prozent im Besitz des ehemaligen Staatschefs Hugo Chavez befand. Geheimdienstberichte weisen darauf hin, dass die Dominion/Bitza-Software in Venezuela mitentwickelt wurde, um die Stimmenauszählung so zu ändern, damit Chávez – und später Staatschef Maduro – garantiert gewännen.

Diese Software sei, so der Experte, auch in zahlreichen anderen Ländern wie Bolivien und den Philippinen eingesetzt worden, um Wahlergebnisse zugunsten eines bestimmten Kandidaten zu fälschen. „In der Folge etablierten Dominion und seine internationalen Partner, darunter Diebold/ES&S (welches später von Dominion übernommen wurde), Scytl und Smartmatic, ein globales Monopol“, so der Experte.

Die Unternehmensstruktur von Dominion und Smartmatic

Dr. Keshavarz-Nia führte weiter aus, dass Dominion aus mehreren Unternehmen zusammensetzt sei, die seine wahren Organisations- und Eigentumsstrukturen verschleierten.

Dazu gehören:

1) Dominion Voting Systems International Corporation, ein Unternehmen aus Barbados;

2) Dominion Voting Systems, Inc., eine Gesellschaft nach dem Recht des Bundesstaates Delaware; und

3) Dominion Voting Systems Corporation, eine kanadische Gesellschaft.

Ähnlich strukturiert ist Smartmatic:

1) Smartmatic International Corporation, ein Unternehmen mit Sitz in Barbados;

2) Smartmatic USA Corporation, eine Gesellschaft nach dem Recht des US-Bundesstaates Delaware;

3) Smartmatic International Holding B.V., ein niederländisches Unternehmen; und

4) Smartmatic TIM Corporation, ein philippinisches Unternehmen.

Dazu sagte der Experte:

> Aus meinen Erfahrungen von der Spionageabwehr für die amerikanischen Geheimdienste schließe ich, dass solche komplexen Unternehmensstrukturen die Beziehungen insbesondere zu Venezuela, China und Kuba verschleiern sollen und es auch erschweren, von Ermittlern entdeckt zu werden.“

Schwerwiegende Sicherheitslücken: Kombination aus kryptografischen Schlüsseln auf gestohlenen USB-Speicherkarten

Die „New York Times“ berichtete im April 2018 über den Informatiker (J.) Alex Hoalderman von der University of Michigan. Er hatte in einem Video demonstriert, wie einfach es ist, eine Dominion-Maschine zu manipulieren. Der Name des Videos lautet „How I Hacked an Election“.

Dominion weigerte sich aber, Mängel im System einzuräumen, geschweige denn diese zu beseitigen. Woraufhin im August 2019 das Wahlsystem ImageCast Precinct komplett gehackt wurde. Dies geschah während der Hacker-Konferenz einer

Gruppe mit Namen „DEF CON Voting Machine Hacking Village“ in Nevada. Die Hacker führten damals vor, wie die Wahlschein-Lesegeräte von Dominion mit einem Schraubenzieher und einer Speicherkarte unterminiert werden konnten.

Dr. Keshavarz-Nia wies darauf hin, dass viele dieser spezifischen Verwundbarkeiten in den Systemen von Dominion, über die schon vor mehr als einem Jahrzehnt beispielsweise in Studien von Kalifornien und Ohio berichtet wurde, auch heute noch in diesen Systemen vorhanden seien.

2019 wurden in Philadelphia ein Laptop und mehrere USB-Speicherkarten, die den kryptografischen Schlüssel zum Zugang zu Dominion Voting-Systemen enthielten, gestohlen. Das Unternehmen bestreitet die Risiken, die mit verlorenen USB-Speicherkarten mit dem kryptographischen Schlüssel verbunden sind. Laut dem Wahlsicherheitsexperten Eddie Perez des überparteilichen OSET-Instituts ist es jedoch

> ganz üblich, dass eine USB-Speicherkarte nicht nur eine Fülle von Informationen enthält, die mit der Gestaltung einer Wahl und deren Wahlscheinen – sowie der Funktionsweise der Wahlautomaten – zusammenhängen, sondern auch interne Systemdaten beinhaltet, die zur Validierung der Wahl verwendet werden“.

Nachdem Dr. Keshavarz-Nia den Inhalt des Dominion Voting-Systems und auch die kryptografischen Schlüssel anderer Wahlsysteme analysiert hatte, sagte er:

> Ich glaube, dass USB-Speicherkarten verwendet wurden, um einen Administrator-Zugang durch eine Hintertür zu erleichtern, um den Wahlvorgang zu durchkreuzen und die Auszählung der Stimmzettel in Pennsylvania, Wisconsin, Michigan, Arizona, Nevada und Georgia zu beeinflussen.“

Abschließend sagte der Cybersicherheitsexperte: „Ich komme zu dem Schluss, dass eine Kombination aus kryptografischen Schlüsseln auf gestohlenen USB-Speicherkarten, schwerwiegenden Sicherheitslücken im System und der Software sowie Hintertüren in den Betriebssystem von Dominion, Scytl und Smartmatic die perfekte Voraussetzung bildeten, um in all den Staaten, wo diese Systeme installiert waren, zu betrügen. Meine Analyse der Daten zur Wahl 2020 zeigt statistische Anomalien gerade bei den Stimmen in den umkämpften Bundesstaaten. Diese Fehler sind weit verbreitet und systemimmanent – und reichen aus, um die Stimmenauszählungen für ungültig zu erklären. Meiner Ansicht nach sind diese Beweise überwältigend und unbestreitbar.“