Strategisches Chaos als Ziel: „Cyberattacken unter falscher Flagge sind die größte Sicherheitsbedrohung bei den Wahlen.“

Kommentar von J.J. Thompson, Senior Director of Global Managed Threat Response bei Sophos zu den Sicherheitsrisiken der anstehenden US-Präsidentschaftswahl.

Angesichts des bevorstehenden Termins zur Wahl des amerikanischen Präsidenten am 3. November ist in den USA eine große Spannung spürbar. Verschärft durch die noch immer wütende Pandemie, die sehr schnell die Wahllandschaft durcheinandergewirbelt hat, und durch Erfahrungen aus 2016, die immer noch in den Köpfen sind, herrscht große Unsicherheit. Dies sind genau die Bedingungen, die sich Cyberangreifer zunutze machen könnten.

Alle Augen blicken auf diese Wahl und mit ihr sind auch Cyberangriffe aller Couleur zu erwarten, von Ransomware-Attacken bis zu direkten Angriffen auf Wahlverwaltungssysteme– von Nationalstaaten bis hin zu gelangweilten Teenagern, die sich beweisen wollen.

Unser erster Impuls ist es meist, Angreifer und ihre Absichten so rasch wie möglich verstehen zu wollen. Doch wir sollten vorsichtig sein, Angriffe zu schnell bestimmten Tätergruppen zuzuordnen. Falsche, vorschnelle Schuldzuweisungen an vermeintliche Urheber von Angriffen, womöglich noch medienwirksam verbreitet, können der Sicherheit einer Wahl genauso schaden, wie die Attacke selbst. Statt womöglich diplomatische Beziehungen zu gefährden, ist es daher ratsamer, sich auf unmittelbare Gegenmaßnahmen zu konzentrieren, um weiteren Schaden während eines Vorfalls zu verhindern.

Die Saat der Zwietracht: Drei Motive hinter Wahlmanipulation
Für den Einsatz angemessener Gegenmaßnahmen ist es wichtig, die Motive der Gegner im Blick zu haben: Bei Wahlmanipulation geht es darum, Macht zu gewinnen, Zwietracht zu säen und Chaos zu stiften. Die Methoden und Vorgehensweisen der Angreifer folgen diesen Motiven und haben drei entsprechende Szenarien zum Ziel:

1. Stören und Verzögern der Wahlergebnisse in Schlüsselbezirken, in denen eine Verzögerung vorteilhaft für das Ergebnis des Gegners sein kann.
2. Öffentliche Zweifel in die Integrität des Wahlergebnisses hervorrufen.
3. Irreführung und Verunsicherung durch gezielte Provokation mittels der falschen Zuordnungen von Angriffen.

Überstürzte Schuldzuweisungen spielen den Gegnern in die Hände
Bei einem aktiven Angriff auf die Wahlsysteme ist die Neutralisierung des aktiven Angriffs zunächst der wichtigste Faktor. Dicht gefolgt von der Vermeidung einer voreiligen Benennung der vermeintlichen Täter. Ein Angriff bleibt ein Angriff. Darum ist es das Wichtigste, sicherzustellen, dass die Wahlen sicher, frei und fair sind, indem man einen Angriff erkennt und darauf reagiert, sobald er stattfindet. Für die Gewährleistung der Integrität der Stimmzettel und um den Wählern Sicherheit zu geben, ist es nicht unbedingt notwendig, umgehend die Identität der hinter dem Angriff stehenden Akteure zu kennen.

Genau hier zeigt sich jedoch ein kritischer Punkt: die unmittelbare Genugtuung ist ein menschlicher Antrieb. Sollten also Berichte über Probleme in der Wahlnacht aufkommen, wird man sofort wissen wollen, wer dafür verantwortlich ist. Dieser Impuls, eilig mit dem Finger zu zeigen und Schuld zuzuweisen, erleichtert es Angreifern umso mehr, Verwirrung und

Misstrauen zu säen – besonders in einer ohnehin schon turbulenten Wahlsaison. Und dies ist eine Strategie, die einige Regierungen nur allzu gerne nutzen wollen.

Gezieltes Chaos unter falscher Flagge – Szenarien und ein echtes Beispiel
Ein anschauliches Beispiel dazu: Nation A möchte in den USA im November Chaos verursachen. Sie möchten natürlich nicht, dass ihnen die Angriffe zugeschrieben werden. Deswegen kompromittieren sie Hosts in Nation B und verwenden diese gehackten Hosts um DDOS-Attacken in der Wahlnacht auf die Wahlreport-Seiten der US-Bundesstaaten zu starten.

Wie wir bei den Ergebnissen der diesjährigen Vorwahlen in Iowa gesehen haben, können langwierige, technisch bedingte Verzögerungen bei der Tabellierung und Berichterstattung der Ergebnisse zu Frustration bei den Wählern und zu einiger Verwirrung darüber führen. Man stelle sich das Szenario in einem der „Swing States" (US-Bundesstaaten, bei denen keine der beiden großen Parteien über eine Mehrheit verfügt) am 3. November vor. Die Verzögerungen könnten Tage oder Wochen der Unsicherheit über die Wahlergebnisse bescheren. Was wäre, wenn in einem betroffenen Staat die Abstimmungen früh endeten und es die Wahlbeteiligung am Abend beeinflusst? Selbst wenn es sich um einen isolierten Vorfall handeln sollte: Wenn sich herausstellt, dass die Wahlberichtsseiten gestört oder gehackt wurden, wird man Angriffsprotokolle einsehen und IP-Adressen finden, die zu Nation 2 zurückverfolgt werden können. Man wird dann wahrscheinlich zu der irrigen Schlussfolgerung gelangen, dass es Nation 2 war, die die Wahl gehackt hat.

Das ist nicht nur eine Hypothese. In 2018, haben russische Hacker Hunderte von Computern und Routern kompromittiert, die mit der Eröffnungszeremonie der Olympischen Winterspiele verbunden waren. Allerdings nutzten sie IP-Adressen aus Nordkorea. Als Ergebnis landete dann auch die erste Anklagewelle vor Nordkoreas Füssen – zumindest in diesem Fall aber scheint dieses Land schuldlos zu sein.

Potenzielle Angriffsflächen im US-Wahlsystem
Wahlen in den USA sind äußerst kompliziert, nicht zuletzt deshalb, weil die Systeme zur Durchführung so dezentralisiert und auf der Ebene der Bundesstaaten und Kommunen zweigeteilt sind. Diese Komplexität zwingt Gegner, viel in die Planung und Koordination von Angriffen zu investieren.

Zu diesem späten Stadium des Wahlzyklus ist es daher sinnvoll, die vielen verschiedenen potenziellen Angriffsflächen in den Wahlsystem zu benennen: Anbieter von Wahlsystemen (sowohl auf menschlicher Ebene als auch auf der Ebene der technischen Infrastruktur/Codes), Registrierung und Elektronische Wahlbücher (e-poll books), die Integrität von Wahlmaschinen, individuelle und/ oder Endanwender Systeme, die in die Wahlverwaltung involviert sind, Stimmenauszählung und Berichtssysteme sowie die Orte, wohin die Wahlergebnisse übermittelt, tabellarisch dargestellt oder veröffentlicht werden – sie alle sind primäre Ziele für Angriffe.

Wir müssen uns auf diese Aspekte konzentrieren:

- Vollständig gepatchte Systeme, ordnungsgemäß konfiguriert und überwacht, Endpoint Protection and Detection-Agenten und -Kontrollen für sämtliche Systeme, die in den Prozess der Tabellarisierung und Übermittlung der Wahlergebnisse involviert sind.
- Einfache, klare und kurz gefasste Richtlinien für die lokalen Wahlhelfer. Umfangreiche Runbooks oder Sicherheitsskripte, die von Regierungsbeamten üblicherweise eingesetzt werden, sind am Wahltag nicht effektiv.
- Bereitstellung verfügbarer Sichtbarkeits-, Untersuchungs- und Reaktions-möglichkeiten, die noch kurzfristig eingerichtet werden können.
- Gewährleistung von hochqualifiziertem Personal, das in der Lage ist, wichtige Signale zu erkennen und darauf zu reagieren, um aktive Bedrohungen schnell neutralisieren zu können.

Oberstes Ziel: Integrität der Wahlsysteme
Cyberkriegsführung ist asymmetrisch: opportune Ziele sind solche, die bemerkbare Störungen verursachen oder besonders verletzliche Informationen oder Zugänge besetzen können. Angreifer benötigen dafür nur eine einzige Schwachstelle. Das Schuld-in-die-Schuhe-schieben-Spiel lenkt unweigerlich den Fokus von diesen deutlich dringenderen Anliegen ab. Letztlich gilt, dass die Zuordnung des ursächlichen Angriffs den Strafverfolgungsbehörden obliegt. Nur sie verfügen über die Legitimation, die Gesetzesverstöße nachzuverfolgen und Anklage gegen Cyberangreifer zu erheben, seien es andere Länder oder Hacker innerhalb der eigenen Grenzen
Für alle anderen – namentlich die Wähler und diejenigen, die für die Überwachung fairer und sicherer Wahlen zuständig sind – muss es in diesen nächsten Tagen in erster Linie darum gehen, die Integrität der Wahlsysteme zu gewährleisten.

Pressekontakt:

Sophos
Jörg Schindler, PR-Manager Central & Eastern Europe
joerg.schindler@sophos.com, +49-721-25516-263

TC Communications
Arno Lücht, +49-8081-954619
Thilo Christ, +49-8081-954617
Ulrike Masztalerz, +49-30-55248198
Ariane Wendt +49-172-4536839
sophos@tc-communications.de