Politische Einflussnahme vor der Bundestagswahl – dem digitalen Bauschaum Paroli bieten

Chester Wisniewski von Sophos zu Wahlmanipulationen mithilfe von Fehlinformationen, Social Engineering oder Hacking – der Sprühschaum bleibt analog.

Das war mal richtig Oldschool in unserer digitalen Welt: Wenige Sekunden benötigten Angreifende, um sozusagen einen analogen Deep Fake zu kreieren: Bauschaum in den Auspuff gesprüht, Aufkleber mit dem Bild des Bündnis 90/Die Grünen-Kanzlerkandidaten Habeck und dem Appell „Sei grüner“ auf den Lack geklebt und schon war beinahe in Echtzeit die Illusion kreiert, dass die Täter wieder einmal Klimaaktivisten waren, die sich diesmal eine Methode überlegt haben, hunderte Autos quasi `ersticken´ zu lassen. Inzwischen häufen sich die Hinweise, dass es hierbei nicht um eine Klimaaktion ging, sondern um den Versuch, Wahlmanipulation zu betreiben. Dahinter verbergen sich, auch das scheint unterdessen klar, russische Interessen. Diese Aktion war also schnell aufzudecken. Anders, auch das wissen wir, sieht es aus, wenn es um technologiebasierte Versuche der politischen Einflussnahme geht.

In der heutigen digital vernetzten Welt werden politische Botschaften und Fehlinformationen immer raffinierter. Manipulationskampagnen, insbesondere solche, die gut finanziert sind, haben erhebliche gesellschaftliche Auswirkungen. Wir sehen Kampagnen, die sich historisch politische und ideologische Ansichten zunutze machen, um Menschen zu überzeugen, zu täuschen und zum (manipulierten) Handeln zu bewegen.

Wir konnten bereits eine Vielzahl von Betrugskampagnen beobachten, in denen generative KI etwa dafür missbraucht wird, um gezielt Nachrichten an ausgewählte Betrugsopfer zu versenden oder anhand von generativen KI-Bildern falsche Social Media-Profile zu erstellen. KI-erstellte Deepfake-Videos sind für das begleitende Social Engineering im Einsatz. Alle Tools werden bereits als Teil politischer Fehlinformation in den sozialen Medien verwendet. Wie das gelingen kann und wie perfekt Cyberkriminelle ihre Täuschungen kreieren, beschreibt ein Artikel des Sophos X-Ops-Teams sehr anschaulich.

Wahlmanipulation ist indes kein neues Phänomen, und es gibt für manipulative Interessensgruppen grundsätzlich zwei Hauptwege, auf denen sie versuchen könnten, Wahlergebnisse zu beeinflussen. Die erste Art der Manipulation konzentriert sich rein auf die Technologie selbst, während die zweite die Technologie einsetzt, um Menschen dazu zu bringen, auf eine Weise zu wählen, die sie sonst vielleicht nicht in Betracht gezogen hätten.

Das Hacken des Systems

Die meisten Länder mit demokratisch gewählten Regierungen haben ihre Wahlsysteme modernisiert, sodass irgendeine Art von Digitalisierung involviert ist. Glücklicherweise hat die Mehrheit der Länder weltweit dem Druck widerstanden, auf Online-Wahlen oder – noch schlimmer – auf die Aufzeichnung von Stimmen in einer Blockchain umzusteigen. Um es klar zu sagen: Die heutige Technologie ist schlichtweg nicht in der Lage, die Identität einer Person zu verifizieren und gleichzeitig die Privatsphäre der Wählenden in einem Online-Mechanismus zu schützen.

In der Regel verlangen Wahlsysteme weltweit, dass Wählende ihre Stimme per Post abgeben oder an einem bestimmten Ort mit speziellen Systemen und Stimmzetteln abstimmen. Dies reduziert die Risiken (die „Angriffsflächen“) für bösartige Hacker – doch Risiken bleiben

bestehen. Die offensichtlichsten Angriffe auf diese Systeme beinhalten Computermalware oder Software-Schwachstellen, die es Angreifenden ermöglichen könnten, das System zu manipulieren. In den meisten Wahlsystemen gibt es drei kritische Punkte, an denen diese Schwachstellen auftreten können:

1. Die Systeme zur Stimmenauszählung
2. Die Systeme zur Verwaltung der Wählerverzeichnisse (die Listen der Personen, die legitim ihre Stimme abgeben dürfen)
3. Die Wahlmaschinen selbst (in Deutschland nicht im Einsatz)

Die wichtigste Verteidigung gegen Malware oder Angriffe auf Sicherheitslücken besteht in der Regel darin, Wahlsysteme nicht mit Netzwerken zu verbinden – und insbesondere niemals direkt mit dem Internet. Diese Strategie, oft als „Air Gap" bezeichnet, verhindert den Fernzugriff auf kritische Systeme. Da Wahlsysteme oft über lange Zeiträume hinweg ungenutzt gelagert werden, ist es außerdem entscheidend, alle Sicherheitsupdates und Software-Patches zu installieren, die vom Hersteller bereitgestellt werden.

Das Hacken der Menschen

Nicht selten, wie sich immer mehr zeigt, besteht die effektivste Methode zur Beeinflussung des demokratischen Prozesses nicht darin, Wahlergebnisse direkt zu manipulieren, sondern Zweifel an deren Richtigkeit zu säen oder Fehlinformationen zu verbreiten, um Wählende in ihrem Entscheidungsprozess zu beeinflussen.

Ein Weg, eine Wahl zu untergraben, könnte darin bestehen, den Auszählungsprozess selbst zu stören, um Verzögerungen zu verursachen. Während Wahlmaschinen selbst in vielen Ländern vom Internet isoliert sind, erfolgt die Stimmenauszählung oder -scannung oft auf handelsüblichen PCs – derselben Hardware, die möglicherweise noch eine Woche zuvor für das Abrufen von E-Mails oder den Kauf von Konzerttickets genutzt wurde. Ein DDoS-Angriff oder das Einschleusen von Malware auf diese Systeme könnte erhebliches Misstrauen in die Wahlergebnisse erzeugen.

Das Verbreiten von Fehlinformationen in sozialen Medien schließlich, kann Menschen dazu verleiten, gegen ihre eigenen Interessen zu handeln – und vor allem die Wahrheit zu ignorieren. Wie eingangs beschrieben können moderne Werkzeuge wie generative KI große Mengen an Desinformation schnell und kostengünstig über verschiedene Plattformen verbreiten.

Durchdachte Maßnahmen zur Risikominderung

Der wichtigste Faktor für die Integrität einer Wahl ist die Möglichkeit, die Ergebnisse zu überprüfen. Kein elektronisches System sollte jemals ohne überprüfbare physische Aufzeichnungen der Wählerstimmen vollständig vertraut werden. Computer können gehackt werden, und das menschliche Gedächtnis ist fehleranfällig – daher ist eine physische Dokumentation der Wählerabsicht entscheidend für das Vertrauen in die Wahlergebnisse.

Radikale Transparenz ist ein wirksames Mittel zur Sicherstellung der Integrität. Alle Abläufe – einschließlich des Computercodes – sollten überprüfbar sein. Zudem braucht es Regeln, um Wahlsysteme nicht nur vor externen Bedrohungen, sondern auch vor böswilligen Insidern zu schützen. Wahlcomputer müssen überprüfbar sein, Software muss als authentisch nachweisbar sein, und Stimmen sollten in nicht-digitaler Form aufgezeichnet werden, um Audits und manuelle Überprüfungen zu ermöglichen.

Angesichts der Vielzahl von Wahllokalen gibt es selten genug technische Experten, um komplexe Fehler sofort zu beheben. Eine einfache Checkliste kann Wahlhelfern helfen, bei Problemen richtig zu reagieren – etwa durch das Trennen des Geräts vom Netzwerk und das sofortige Benachrichtigen der Wahlbehörden.

Fazit

Es bleibt dabei: Technologie wird zunehmend eine Rolle bei Wahlen und Wahlkampagnen spielen. Es ist wichtig, ihre Vorteile für Offenheit, Effizienz und Zugänglichkeit zu nutzen. Durch transparente Prozesse, sinnvolle Sicherheitsmaßnahmen und sorgfältige Protokollierung können Regierungen Technologie sicher für Wahlen einsetzen.

Die größere Herausforderung liegt in den sozialen Risiken: der massenhaften Verbreitung von Fehlinformationen. Durchdachte Regulierung, Forschung zu Erkennungsmethoden und Kooperationen mit Plattformbetreibern sind erforderlich, um die Verbreitung von computergenerierten Lügen einzudämmen – und den digitalen Bauschaum zu entlarven.

Chester Wisniewski ist Global Field CTO bei Sophos

Social Media von Sophos für die Presse
Wir haben speziell für Sie als Journalist*in unsere Social-Media-Kanäle angepasst und aufgebaut. Hier tauschen wir uns gerne mit Ihnen aus. Wir bieten Ihnen Statements, Beiträge und Meinungen zu aktuellen Themen und natürlich den direkten Kontakt zu den Sophos Security-Spezialisten.

Folgen Sie uns auf und

LinkedIn: https://www.linkedin.com/groups/9054356/
X/Twitter: @sophos_info

Pressekontakt:

Sophos
Jörg Schindler, Senior PR-Manager EMEA Central
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