Der Computer als Wahlhelfer – Fluch oder Segen?

„Technologie ist ein zunehmend wichtiger Teil aller Wahl- und Wahlkampfprozesse weltweit - und damit ein zentraler Faktor, um die Offenheit, Effizienz und Zugänglichkeit unserer Demokratien zu gewährleisten. Allerdings hat diese Entwicklung Schattenseiten, da böswilligen Akteuren immer mehr Wege zur Verfügung stehen, um sowohl die Technik als auch die Menschen zu manipulieren. Ein möglicher Ausweg aus dieser Misere ist tiefgreifende Transparenz.“

Ein Kommentar von Chet Wisniewski, Field CTO bei Sophos

Es scheint, dass alles, was gehackt werden kann, gehackt wird. Tatsächlich ist die zunehmende Automatisierung in Sachen Cyberkriminalität ein Grund dafür, dass kaum noch digitale Systeme, die in irgendeiner Form am Tropf der Onlinewelt hängen, sicher vor Attacken sind. Umso problematischer wird diese Entwicklung, wenn die Folgen einer Manipulation weitreichend sind – wie zum Beispiel bei Wahlen.

In den meisten Ländern mit demokratisch gewählten Regierungen haben wir unsere Wahlsysteme dahingehend modernisiert, dass sie je nach Land mehr oder weniger mehr stark computerisiert sind. Diese Modernisierung kann so einfach sein wie der Einsatz von Scannern zur Auszählung papierbasierter Stimmzettel oder so komplex wie der Kauf und die Wartung vollständig per Computer betriebener Wahlgeräte. Daher ist es für viele nur eine Frage der Zeit, bis es zur nächsten Schlagzeile über gehackte Wahlen kommt.

Glücklicherweise haben wir uns auf der ganzen Welt größtenteils gegen den Drang gewehrt, komplett auf Online-Abstimmungen umzusteigen oder, schlimmer noch, Stimmzettel in einer Blockchain aufzuzeichnen. Ehrlich gesagt ist die Technologie, über die wir aktuell verfügen, einfach nicht in der Lage, die Identität einer Person zu überprüfen und die Privatsphäre des Wählers durch einen Online-Mechanismus zu schützen. Allerdings bieten momentan genutzte Technologien böswillig motivierten Gruppierungen durchaus Möglichkeiten Wahlergebnisse zu manipulieren – primär in zwei Varianten: Die erste Art der Manipulation konzentriert sich ausschließlich auf die Technologie selbst, während die zweite Strategie sich darauf konzentriert, Menschen zu manipulieren, auf eine Weise zu wählen, die sie so nicht vorhatten.

Das System manipulieren

Bei den meisten Wahlsystemen auf der ganzen Welt müssen Teilnehmer ihren Stimmzettel per Post einsenden oder ihre Stimme an einem bestimmten Ort über spezielle Systeme und Stimmzettel abgeben. Dies verringert zwar die Angriffsflächen für böswillige Hacker enorm, birgt aber dennoch Risiken. Die offensichtlichste Art von Angriffen auf diese dedizierten Systeme sind Computerviren oder die Ausnutzung von Software-Schwachstellen, um manipulativ einzugreifen. Im Wesentlichen betrifft diese Gefahr drei Bereiche: die Wahlgeräte selbst (sofern sie elektronisch sind), die Systeme zur Stimmenauszählung und die Systeme zur Verwaltung der Wählerverzeichnisse.

In den meisten Situationen besteht die primäre Verteidigung gegen Angriffe einfach darin, Abstimmungssysteme überhaupt nicht mit Netzwerken und schon gar nicht direkt mit dem Internet zu verbinden. Dieser oft als „Air Gap“ bezeichnete Ansatz verhindert den Fernzugriff auf kritische Systeme. Um Air-Gap-Systeme anzugreifen, benötigt ein Angreifer physischen Zugriff auf jedes Zielgerät, was einen Missbrauch im großen Stil grundsätzlich verhindert. Aber natürlich müssen elektronische Geräte zur Stimmabgabe für Wähler physisch zugänglich sein, genauso wie Geräte zur Stimmauszählung für Wahlhelfer – und damit potenziell auch für kriminell motivierte Personen. Es handelt sich also nicht um eine universelle Lösung.

Der zweite wichtige Aspekt zur Absicherung von Wahlsystemen ist das Einspielen von Fixes und Software-Updates. Dieser eigentlich selbstverständliche Prozess ist besonders wichtig, da die Wahlsysteme zwischen den Wahlen häufig für längere Zeiträume nicht genutzt werden. Doch auch hier lässt sich eine positive Entwicklung feststellen. Abstimmungssysteme werden häufiger aktualisiert, nicht zuletzt aufgrund von aufmerksamkeitsstarken Wettbewerben wie das Voting Village auf der Hackerkonferenz DEF CON, das damit begonnen hat, diese Systeme auf Schwachstellen zu untersuchen und Anbieter unter Druck zu setzen, sie besser abzusichern. Hier ist es essenziell, dass auch der Update-Management-Prozess dahingehend gestaltet sein muss, dass die Legitimität von Patches sichergestellt ist.

Die Menschen manipulieren

Nicht selten besteht die beste Möglichkeit, in den demokratischen Prozess einzugreifen, nicht darin, das Wahlergebnis direkt zu ändern, sondern darin, das Misstrauen gegenüber der Richtigkeit der Ergebnisse zu schüren oder Desinformationen zu verbreiten, die darauf abzielen, die Entscheidungen der Wähler am Wahltag zu ändern. Heutzutage kann ein Großteil dieser Meinungsbeeinflussung mit technologischen Mitteln erledigt werden, was die Realisierung solcher manipulativen Operationen im großen Maßstab relativ einfach und kostengünstig macht.

Eine Möglichkeit, das Vertrauen in den rechtmäßigen Ablauf einer Wahl zu senken, besteht darin, in den Prozess der Stimmenauszählung einzugreifen und dadurch Verzögerungen zu verursachen. Während Wahlgeräte selbst oft vom Internet zu isoliert sind, erfolgt die Tabellierung oder das Scannen von Stimmzetteln oftmals auf alltäglichen PCs, mit denen letzte Woche noch E-Mails beantwortet oder Taylor-Swift-Tickets gekauft wurden. Die Durchführung eines DDoS-Angriffs oder das Einschleusen von Schadsoftware auf diese Systeme ist für Hacker häufig praktischer als der Angriff auf Wahlmaschinen und kann schnell zu einem Vertrauensverlust in die Wahlergebnisse führen. Ein Eingriff in diese Technologieketten und die Bekanntmachung kann leicht dazu führen, dass Menschen die Richtigkeit der Stimmauszählung anzweifeln.

Schließlich kann die bloße Verbreitung von Fehlinformationen in den sozialen Medien ahnungslose Menschen dazu verleiten, sich gegen ihre eigenen Interessen zu wenden und, was noch wichtiger ist, der Wahrheit den Rücken zu kehren. Durch den Einsatz moderner Tools wie generativer KI (z. B. ChatGPT oder Bard) wird die Möglichkeit, Desinformationen mit geringfügigen Variationen massenhaft über Social-Media-Plattformen zu verbreiten, kostengünstig und effektiv. Die breite Streuung verleiht den manipulativen News alleine durch ihren Umfang und den Anschein breiter Akzeptanz eine hohe Glaubwürdigkeit. Unsere eigenen Forscher bei Sophos AI haben auf der DEFCON 31 demonstriert, dass generative KI genutzt werden kann, um den Aufbau einer groß angelegten Manipulation zu automatisieren.

Es gilt zudem zu Bedenken, dass Desinformation keinen bestimmten Kandidaten oder ein bestimmtes Thema direkt unterstützen oder verunglimpfen müssen. Eines der wiederkehrenden Desinformationsmuster der letzten Jahre zielt lediglich auf Wähler bestimmter Bevölkerungsgruppen oder Wahltendenzen ab und versorgt sie z.B. mit Fehlinformationen über den Tag, den Ort oder die Registrierungsnachweisanforderungen für ihre Wahlen.

Das Vertrauen in Wahlen aufrechterhalten

Das Wichtigste zur Wahrung der Integrität einer Wahl ist die Möglichkeit, die Ergebnisse nachvollziehbar überprüfen zu können. Ohne überprüfbare physische Aufzeichnungen, die von Menschen manuell kontrolliert werden können, sollte keinem elektronisches System jemals vollständig vertraut werden. Computer können gehackt werden und das menschliche Gedächtnis ist bekanntermaßen fehlbar. Daher ist es für die Gesellschaft von entscheidender Bedeutung, die Absichten eines Wählers physisch zu dokumentieren, um die Legitimität der Ergebnisse zu ermöglichen.

Zudem kann radikale Transparenz ein erstaunliches Antiseptikum sein. Alle Verfahren und Prozesse, einschließlich des Programmcodes, wenn Computer beteiligt sind, sollten öffentlich zugänglich und überprüfbar sein, um ihre Integrität sicherzustellen. Das bedeutet nicht, dass die gesamte Software Open Source sein muss, aber wenn nötig, muss bestätigt werden können, dass sie frei von Hintertüren ist und wie angegeben funktioniert. Grundsätzlich sollte auf die Möglichkeit einer Überprüfung bestanden werden, ob ein angewendeter Patch digital signiert und authentisch vom Anbieter stammt, und es sollte die Möglichkeit bestehen, Code wichtiger Programme auf Schwachstellen und Hintertüren zu überprüfen.

Computer sind fehleranfällig - aus den unterschiedlichsten Gründen. Wenn wir also Computer im Rahmen von Wahlen verwenden, ist es wichtig, sie so zu konfigurieren, dass ein vollständiger Prüfpfad ihres Verhaltens erstellt werden kann. Zudem muss ein einfach durchzuführendes Verfahren festgelegt sein, das bei einem Verdacht, dass Systeme aufgrund von Hackerangriffen oder aus anderen Gründen nicht richtig funktionieren, es ermöglicht die Prozesse, die zum Fehler führten, nachvollziehen zu können. Entsprechend sollte auf allen Computern, die zum Aufzeichnen oder Tabellieren von Abstimmungen verwendet werden, eine erweiterte Erkennungs- und Reaktionssoftware (XDR) installiert sein, um jede auf dem Gerät durchgeführte Aktion sorgfältig zu protokollieren. Dies hilft im Fall der Fälle bei der forensischen Analyse und liefert die Informationen, die zur Ermittlung der Ursache für abnormales Verhalten erforderlich sind.

Technologie wird zunehmend ein Teil aller Wahl- und Wahlkampfprozesse sein und ist ein wichtiger Faktor um die Offenheit, Effizienz und Zugänglichkeit unserer Demokratien zu gewährleisten. Durch die Einführung transparenter Prozesse, umsichtiger und klarer Sicherheitsmaßnahmen und einer detaillierten Protokollierung automatisierter Prozesse können wir Technologie nutzen, um unsere Wahlen sicher zu unterstützen.

Das schwieriger zu bewältigende Risiko sind die Auswirkungen der zunehmenden Verbreitung von professionell gestalteten Fehlinformationen durch neue Technologien wie künstliche Intelligenz. Diese Entwicklung erfordert eine durchdachte Regulierung, sorgfältige Forschung zu Erkennungsmethoden und die Zusammenarbeit mit den Betreibern von Kommunikationsplattformen, um konzertierte Anstrengungen zu unternehmen, computergenerierte Falschmeldungen einzudämmen.

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, 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