IPG

KOMMENTAR 27.04.2017 | Martin Schallbruch

Die Sicherheit Deutschlands wird auch im Internet verteidigt

Cyberangriffe könnten die Bundestagswahl manipulieren. Wir müssen Parlament und Parteien endlich als kritische Infrastruktur begreifen.

Kann die Bundestagswahl durch Cyberangriffe manipuliert werden? Spätestens seit der US-amerikanischen Präsidentschaftswahl wird diese Frage in der Öffentlichkeit und im politischen Raum heftig diskutiert. Dabei ist die Antwort einfach: Ja, natürlich kann die Bundestagswahl digital manipuliert werden. Kann eine solche Manipulation wahlentscheidend sein? Wir wissen es nicht.

Die Digitalisierung von Staat und Wirtschaft, von Gesellschaft und Alltagsleben beginnt nicht erst, sie ist weit fortgeschritten. Jedes komplexe System hängt von digitaler Technik ab, von der Energieversorgung bis zum Gesundheitswesen. Das gilt selbstredend auch für das politische System. Und digitale Technik ist alles andere als sicher. Über die letzten zehn Jahre hat sich die Zahl der Schwachstellen in den wichtigsten 50 Softwareprodukten nicht verringert, sondern erhöht. Das technische Angriffsrisiko wird durch die gestiegene Komplexität der IT-Systeme weiter erhöht: Der Einsatz mobiler Geräte, die Datenspeicherung in der *Cloud* und die Vernetzung von Alltagsgegenständen (Internet of Things) haben eine Komplexität erzeugt, die Angreifer ausnutzen und die Verteidiger (also die Betreiber der IT-Systeme) nur schwer absichern können. Gleichzeitig ist die Abhängigkeit von digitaler Technik gewachsen, so auch die Abhängigkeit des politischen Systems. Staatliche Dienstleistungen, der Betrieb der Medienunternehmen, die Meinungsbildung in den Parteien, die demokratische Partizipation – all das findet zunehmend digital statt. Digitalisierung und Abhängigkeit von digitaler Technik schreiten in einer Geschwindigkeit voran, mit der die IT-Sicherheit nicht Schritt halten kann.

Über die letzten zehn Jahre hat sich die Zahl der

Die Vorfälle rund um die US-Präsidentschaftswahlen zeigen, welches Potenzial dieser gefährliche Mix für die

Schwachstellen in den wichtigsten 50 Softwareprodukten nicht verringert, sondern erhöht.

Manipulation von Wahlen haben kann. Der Einsatz von Social Bots zur Manipulation der öffentlichen Meinung, das Entwenden von Daten aus den schlecht gesicherten IT-Systemen der Parteien oder auch der (behauptete) Versuch der Manipulation von Wahlgeräten und Wahlverfahren beschreiben eine ganze Palette von Möglichkeiten für ausländische Nachrichtendienste oder andere Interessengruppen, Einfluss auf Wahlergebnisse zu nehmen.

Cyberangriffe auf das Wahlsystem

Wahlen werden in Deutschland im Wesentlichen durch die Kommunen durchgeführt. Die eigentliche Wahlhandlung findet bislang nicht digital statt. Versuche zur Einführung von Wahlcomputern wurden durch eine Entscheidung des Bundesverfassungsgerichts von 2009 gestoppt. Die Hürde für Wahlcomputer wurde aufgrund der Manipulationsmöglichkeiten so hoch gelegt, dass man seitdem auf ihren Einsatz verzichtet. Manipulationsmöglichkeiten bestehen allerdings bei der Auswertung der Wahlergebnisse. Der Bundeswahlleiter und seine IT-Infrastruktur dürften durch das Bundesamt für Sicherheit in der Informationstechnik gut geschützt sein. Auch in den Bundesländern wird viel Aufmerksamkeit auf die Sicherheit der zentralen Systeme gelegt. Im Bereich der Kommunen sind Cyberangriffe allerdings kaum auszuschließen. Zu unterschiedlich ist die verwendete IT-Infrastruktur, zu wenig Wissen über IT-Sicherheit existiert bei den zuständigen Behörden. Es ist dringend erforderlich, dass die Landesregierungen größere Anstrengungen unternehmen, die IT-Systeme der Kommunen gegen Angriffe zu schützen und die Gemeinden mit entsprechender Expertise zu unterstützen.

Cyberangriffe auf das politische System

Auch das politische System mit Parlamenten und Parteien ist anfällig für Cyberangriffe. Abflüsse von Daten, wie beim US-amerikanischen „Democratic National Committee“, sind auch in Deutschland nicht auszuschließen. Der erfolgreiche Angriff auf Abgeordnete des Deutschen Bundestages im Jahr 2015 zeigt dies. Auch die IT-Infrastruktur der Parteien ist zu heterogen und zu wenig von Spezialisten geschützt, als dass man Angriffe ausschließen könnte. Das aus solchen Angriffen gewonnene Material kann zu vielerlei Zwecken eingesetzt werden: zur Erpressung betroffener Politiker, zu ihrer öffentlichen Diskreditierung oder zur Manipulation der Meinungsbildung einer Partei oder gar der

öffentlichen Meinung. Es ist an der Zeit, dass wir unser politisches System einschließlich der Parlamente und Parteien als kritische Infrastruktur begreifen und harte Vorgaben für die IT-Sicherheit auch dieses Bereichs erlassen. Das im Jahr 2015 verabschiedete Gesetz über IT-Sicherheit zwingt zwar Banken und Versicherungen, Energiewirtschaft, Krankenhäuser oder Paketzusteller zu Sicherheitsauflagen für ihre Systeme, nicht aber den Bundestag, die Landtage oder die politischen Parteien. Das Bundesamt für Sicherheit in der Informationstechnik (BSI) wird hier nur auf Anforderung und nur beratend tätig. Das muss sich ändern.

Digitale Manipulation der demokratischen Öffentlichkeit

Da politische Meinungs- und Willensbildung zunehmend auf digitalen Plattformen wie Facebook oder Twitter erfolgt, ist hier neue manipulative Einflussnahme möglich. Ein Beispiel sind die *Social Bots*. Dabei handelt es sich um automatische Verfahren innerhalb der Plattformen, die bestimmte Meinungen (oder auch Falschbehauptungen) so verbreiten, dass sie überproportional wahrgenommen werden und damit die Debatte beeinflussen. *Social Bots* nutzen aus, dass im Internet nicht ohne weiteres erkennbar ist, ob ein Mensch die Nachricht verschickt oder teilt oder ob dies eine Maschine, ein digitaler „Verstärker“ tut. *Social Bots* sind nicht per se problematisch oder gefährlich. Die Einflussnahme von *Bots* auf die Öffentlichkeit muss aber transparent gemacht werden. Soziale Netzwerke spielen eine maßgebliche Rolle für unser digitales öffentliches Leben. Welche Mechanismen dort wirken und wie sie genutzt werden, sollte für die Öffentlichkeit erkennbar sein. Facebook, Twitter und andere Dienste sollten verpflichtet werden, Hilfsmittel zur Verfügung zu stellen, damit Journalisten und Forscher erkennen und auswerten können, wo Meinung manipuliert wird.

Auch das politische System mit Parlamenten und Parteien ist anfällig für Cyberangriffe.

Die digitale Gesellschaft bietet Chancen, auch für unser demokratisches System. Aber sie bietet eben auch neue Manipulationsmöglichkeiten. Deutschland sollte dies nicht auf die leichte Schulter nehmen. „Wehrhafte Demokratie“ erfordert auch im Netz ein konsequentes und entschlossenes Verteidigen unseres demokratischen Systems.



Martin Schallbruch

Martin Schallbruch ist stellvertrender Direktor des Digital Society Institute der ESMT Berlin und war bis 2016 Abteilungsleiter für Cybersicherheit im Bundesministerium des Innern.

-