Cyber-Attacken

Wahl in Gefahr?

[14.09.2017] Ist Wahl-Software ein Einfallstor, über das Hacker die Ergebnisse der Bundestagswahl manipulieren können? Das Unternehmen Malwarebytes hält dieses Szenario für eher unwahrscheinlich. Dennoch sei die Gefahr, die von Cyber-Angriffen im Umfeld der Wahlen ausgehe, nicht zu unterschätzen.

Über Sicherheitslücken beim Einsatz von Wahl-Software haben vor Kurzem verschiedene Medien berichtet. Der Hintergrund: Hacker des Chaos Computer Clubs (CCC) haben die in mehreren Bundesländern zur Erfassung und Auswertung der kommenden Bundestagswahl verwendete Software PC Wahl des Anbieters vote iT auf Angriffsmöglichkeiten untersucht. Die Analyse ergab laut dem CCC eine Vielzahl von Schwachstellen und mehrere mögliche Angriffsszenarien. Diese würden die Manipulation von Wahlergebnissen auch über die Grenzen von Wahlkreisen und Bundesländern hinweg erlauben.

Updates erhöhen Sicherheit

Das Bundesamt für Sicherheit in der Informationstechnik (BSI) und Hersteller vote iT haben dazu bereits Stellung genommen: Man habe in intensiver Zusammenarbeit mit den zuständigen Bundes- und Landeswahlleitern Empfehlungen zur Verbesserung des Sicherheitsniveaus bei der Übermittlung vorläufiger Wahlergebnisse mit der genannten Software ausgesprochen. Hersteller vote iT ist dabei, die BSI-Empfehlungen umzusetzen und stellt diese im Rahmen von Updates auf seiner Website zur Verfügung. So sei unter anderem die Sicherheit der Software-Verteilung durch Optimierungen an der eingesetzten Infrastruktur und durch veränderte Prozesse verbessert worden. Um Manipulationen von PC-Wahl oder der Software-Updates zu unterbinden, werden künftig zudem nur noch digital signierte Update-Pakete verarbeitet. Nutzer der Software können somit laut vote iT überprüfen, ob die Software tatsächlich vom Hersteller stammt und im Originalzustand vorliegt. Den kommunalen Anwendern wird nun dringend empfohlen, die Updates auch durchzuführen. Daneben sind auf Anraten des BSI weitere organisatorische Prozesse implementiert worden, welche die Sicherheit bei der Übermittlung der Wahlergebnisse verbessern.
Es gilt in diesem Fall aber auch: Es wird nicht so heiß gegessen, wie gekocht wird. So kann etwa vote iT nach eigenen Angaben die Aussage des Chaos Computer Clubs, dass es möglich sei, die Software PC Wahl so zu manipulieren, dass nach Belieben eigene Versandpakete mit Stimmdaten erstellt und in den Wahlprozess eingespeist werden könnten, nicht nachvollziehen, da der Einsatz der Software lokal bei den Städten und Gemeinden erfolgt und die Meldungsprozesse in der Regel in internen Netzen – teilweise kommunalen Landesnetzen – stattfinden und von Mitarbeitern in den Wahlämtern auf unterschiedlichsten Wegen in den jeweiligen Bundesländern vorgenommen werden. „Da die bei den Städten und Gemeinden genutzten Software-Pakete nach allen uns vorliegenden Informationen nicht kompromittiert sind, hat das keine Konsequenzen für die Nutzung von PC Wahl“, so vote iT abschließend.

Manipulation eher unwahrscheinlich

Dass Hacker-Attacken auf Computer-Systeme im Umfeld der Wahlen zwar durchaus vorstellbar sind, sagt auch Helge Husemann, Product Marketing Manager EMEA bei dem Cybersecurity-Unternehmen Malwarebytes. Dass eine tatsächliche Manipulation der Wahlergebnisse gelingt, ist ihm zufolge aber eher unwahrscheinlich, da die Auszählung und Dokumentation der Stimmzettel papiergebunden bleibe. Die

telefonische Schnellmeldung der Kommunen stelle eine weitere Sicherheitsstufe dar. Dennoch sei das Risiko von Cyber-Angriffen nicht zu unterschätzen, warnt der Experte von Malwarebytes. Neben Hacker-Attacken gehen nach Angaben von Helge Husemann die größten potenziellen Gefahren von der Veröffentlichung sensibler Informationen, Fake Leaks und Malware-Kampagnen aus.

Leaks und Malware-Kampagnen möglich

So haben beim Bundestag-Hack im Mai 2015 Cyber-Kriminelle einen 16 Gigabyte-großen Datensatz vom Hauptserver des Deutschen Bundestag abgegriffen. Nach Angaben von Malwarebytes könnten demnach in der heißen Wahlkampfphase kurz vor der Wahl streng geheime oder persönliche Daten bekannt werden, die den Parteien und ihren Kandidaten massiv schaden können. Eine Gefahr stellen auch so genannte Leaks dar, wie sie etwa bei der französischen Wahl stattfanden. Hierbei seien E-Mails und persönliche Daten des jetzigen Präsidenten Emmanuel Macron offengelegt worden, um ihm zu schaden. Noch schlimmer: Cyber-Kriminelle seien auch in der Lage, belastendes Material zu fälschen, meint Helge Husemann. Außenstehende könnten dabei kaum einen Unterschied ausmachen, und nicht erkennen, ob eine E-Mail von Bundeskanzlerin Angela Merkel wirklich den kompromittierenden Inhalt enthält, den sie vorgibt. Die Bundestagswahl eignet sich nach Angaben von Husemann auch optimal, um die breite Wählerschaft anzugreifen. Ein durchaus plausibles Szenario sei etwa, dass sich Kriminelle der E-Mail-Kampagnen der Parteien bedienen und Links austauschen, die dann anstatt auf das Wahlprogramm auf Web-Seiten mit Schad-Software führen.
Sein Fazit: Trotz der relativ gut abgesicherten Bundestagswahl sind Cyber-Kriminelle ständig auf der Suche nach neuen Sicherheitslücken. Zwar sind vor allem politische Institutionen gefährdet, doch auch Privatpersonen können ins Visier geraten. Daher gilt für alle: Sensible Daten sollten immer nach dem neuesten Stand der Technik geschützt werden.

(bs)

Zur Analyse des CCC

Stichwörter: IT-Sicherheit, Wahlen, Malwarebytes