Die Kommunalwahl ist sicher.

Bei der Kommunalwahl am 14. März 2021 wird auch im Hinblick auf die IT-Sicherheit Vorsorge getroffen. Von allen Beteiligten wird erwartet, dass sie das Notwendige und Mögliche veranlassen. Schwierigkeiten mit der eingesetzten Software wie bei der bayerischen Kommunalwahl wird es in Hessen nicht geben.

Dass Computersystem „gehackt“ werden können, ist keine Spezialität von Wahlen, sondern eine allgemeine Tatsache. Kommunen und IT-Dienstleister bereiten sich aber unter Beachtung der IT-fachlichen Standards auf die Wahlen vor. Wahlen sind am wenigsten für Hackerangriffe anfällig, weil die Ergebnisermittlung anhand der Stimmzettel überprüft werden kann.

Nachstehend einige Antworten auf Fragen, die aktuell bezüglich der von den hessischen Kommunen eingesetzten Wahlsoftware öffentlich gestellt wurden:

Frage: Kann ein Angreifer das Wahlergebnis manipulieren, wenn ein Wahlhelfer mit dem Auszählrechner im Internet surft und auf einen bösartigen Link klickt?

Antwort *(ekom21): Ein Angriff durch einen bösartigen Link wird Cross-Site-Scripting-Attacke (CSRF) genannt. Zur Vermeidung dieser Angriffe wurden sogenannte CSRF-Token eingeführt. Diese Token werden vom Server an den Browser geschickt und müssen beim Rückversand an den Server übereinstimmen. Diese Token sind dem Angreifer nicht bekannt, da sie sich permanent verändern.*

Frage: Können Angreifer über das lokale Netzwerk mit geringem Aufwand Manipulationen direkt an der Datenbank vornehmen? Gibt es hier Sicherheitslücken

Antwort *(ekom21)**: Die Datenbank wird durch den Betreiber so konfiguriert, dass ein Zugriff nur vom Server, auf dem die Stimmzettelerfassung läuft, möglich ist. Damit ist die Manipulation im Netzwerk ausgeschlossen.*

Frage: Soll die Software in Hessen, anders als in Bayern, ausschließlich zentral auf Servern installiert werden?

Antwort *(ekom21)**: In Hessen sollen ausschließlich Serverinstallationen in Betrieb genommen werden.*

Frage: Können die Wahlergebnisse bei einer Verwendung von USB-Sticks leicht verfälscht werden? Wenn solche USB-Sticks verwendet werden, müssen sie dann eine Signatur haben?

Antwort *(ekom21)**: USB-Sticks werden bei der Kommunalwahl in Hessen aus Sicherheitsgründen nicht eingesetzt.*

Frage: Stimmt es, dass das Programm die Zugriffsrechte des jeweiligen Nutzers nicht ausreichend kontrolliert und jeder Wahlhelfer deshalb auf Administratoren-Funktionen wie das Löschen des lokalen Wahlergebnisses zugreifen kann?

***Antwort** (ekom21)**:** Es gab bei der bayerischen Kommunalwahl zwei Funktionen, bei denen die Überprüfung nicht korrekt war. Hier wurde eine Programmänderung vorgenommen.*

Frage: Kann es in Hessen wie offenbar in Bayern Probleme beim Import und Export der Ergebnisse geben, insbesondere wenn eine Datei so groß ist, dass sie einfach nicht auf einen anderen Rechner importiert werden kann?

***Antwort** (ekom21)**:** Dieses Problem trat nur in der USB-Variante auf, die in Hessen nicht zum Einsatz kommt.*

Frage: Können unzureichende Vorbereitungen durch Tests der Software im Vorfeld aufgedeckt werden? Werden solche Tests veranlasst?

***Antwort** (ekom21)**:** In der Software wird ein Assistent angeboten, der die Konfiguration im Rahmen des technisch Machbaren überprüft. Am 9. und 10. Februar wird ein hessenweiter Wahltest durchgeführt. Auch hier können sich Hinweise zur Optimierung ergeben.*

Weiterhin wird der Votemanager im Auftrag des Software-Herstellers aktuell durch ein externes Unternehmen nach den OWASP-Kriterien (Open Web-Application Security Project) überprüft. Diese Tests erfolgen in Ergänzung zu den bestehenden kontinuierlichen Qualitätssicherungsmaßnahmen. Über die Ergebnisse wird die ekom21 zeitnah vor der Kommunalwahl in Hessen unterrichtet.

Frage: Hat die ekom21 zur Verbesserung der IT-Sicherheit sog. Penetrationstests vorgenommen) Was genau versteht man darunter? Was sind die Ergebnisse dieser Tests?

***Antwort** (ekom21)**:** Ein Penetrationstest wird noch durchgeführt. Hiermit wird ein unabhängiges Unternehmen beauftragt, evtl. auftretende Schwachstellen werden umgehend beseitigt. Ein Penetrationstest, kurz Pentest, ist ein umfassender Sicherheitstest mit dem möglichst alle Systembestandteile und Anwendungen eines Netzwerks und/oder eines Softwaresystems geprüft werden. Dabei kommen die gleichen Mittel und Methoden zur Anwendung, die ein Angreifer (ugs. „Hacker“) anwenden würde, um unautorisiert in das System einzudringen (Penetration).*

Frage: Wird die ekom21 den Kommunen noch Hinweise zur IT-Sicherheit beim Betrieb der Software geben?

***Antwort** (ekom21)**:** Die Kommunen sind schon über die IT-Sicherheit informiert worden. Bei entsprechendem Anlass werden weitere Informationen gegeben.*

Frage: Wie wird bei und nach der Wahl überprüft, ob alles mit rechten Dingen vorging? Kann man bei Verdacht auf Fehler bei der Ergebnisermittlung nachzählen

***Antwort**: Nach der Wahl wird in einem Wahlprüfungsverfahren geprüft, ob es bei der Wahl zu ergebnisrelevanten Unregelmäßigkeiten gekommen ist. Das Verfahren erfolgt auf Einspruch und von Amts wegen; zuständig sind erstinstanzlich die jeweiligen neu gewählten Vertretungskörperschaften. In schwierigen Fällen besteht die Möglichkeit, dass die Gemeindevertretung oder der Kreistag einen eigenen Wahlprüfungsausschuss bildet. Bestehen substantiierte Anhaltspunkte, dass es im Rahmen der Ergebnisermittlung zu Unregelmäßigkeiten gekommen ist, muss die Gemeindevertretung diesen nachgehen. Auch eine Nachzählung von Stimmen kann nur bei substantiierten Anhaltspunkten für Unregelmäßigkeiten erfolgen; ein knapper Wahlausgang oder ein bloßer Verdacht auf Fehler führen nicht zu einer erneuten Zählung von Stimmen.*

Frage: Sollte es besser gesetzliche Vorgaben für die Zulassung von Wahlsoftware geben? Kann man so etwas gesetzlich regeln?

***Antwort**: Nach § 48a Abs. 8 Satz 1 Kommunalwahlordnung kann die Stimmermittlung auch mit automatisierten Verfahren erfolgen, wenn dabei Sicherheit und Zuverlässigkeit bei der Ermittlung und Feststellung des Wahlergebnisses gewährleistet sind. Die Prüfung dieser Voraussetzungen obliegt zunächst den Kommunen, die automatisierte Verfahren einsetzen wollen. Diese sind vor einem Einsatz von automatisierten Verfahren insbesondere verpflichtet, eine dem jeweiligen Stand der Technik entsprechende Sicherheit zu gewährleisten und Vorgaben des Herstellers zur Betriebsumgebung zu beachten. In einem Schreiben an die Kommunen wurde zusätzlich empfohlen, anhand ausgesuchter Stimmzettelbeispiele die Funktionsfähigkeit einer Software vor dem Einsatz zu überprüfen und nach einer bestimmten Anzahl von Stimmzetteln das Ergebnis noch händisch zu ermitteln und kontrollieren. Erst wenn der Wahlvorstand, dem die Ergebnisermittlung obliegt, von der richtigen Funktion des eingesetzten Verfahrens überzeugt ist, kann eine Stimmermittlung mit automatisierten Verfahren erfolgen.*