LANDTAG NORDRHEIN-WESTFALEN
16. Wahlperiode

Drucksache **16/13464**

15.11.2016

Antwort

der Landesregierung

auf die Kleine Anfrage 5245 vom 13. Oktober 2016
des Abgeordneten Robert Stein CDU
Drucksache 16/13203

Wie steht es um die Straßenverkehrssicherheit im digitalen Zeitalter: Werden sensible Infrastrukturbereiche hinreichend geschützt und Einfallstore geschlossen?

Vorbemerkung der Kleinen Anfrage

Der Begriff Smart City steht für ein gesamtheitliches Entwicklungskonzept welches darauf abzielt, Städte technologisch fortschrittlicher und effizienter in unserer digitalisierten Welt zu gestalten. Die intelligente Vernetzung von Geräten schafft durch Synergien und eine zentrale Steuerung einen Mehrwert für die Städte und ihre Bürger. Unter diesen Sammelbegriff fallen beispielsweise Konzepte wie das smart parking, smart traffic oder auch smart shopping.

Diese zunehmende Vernetzung birgt allerdings auch große Gefahren, wenn unzureichende Schutzmaßnahmen getroffen werden. Die Infrastruktur der Smart Cities entwickelt sich schneller als die Mittel zu ihrem Schutz. Diese sensiblen Systeme können Ziel von Hackern werden, die die Ordnung und Orientierung in einer Stadt komplett durcheinander bringen können (vgl. https://de.securelist.com/analysis/veroffentlichungen/71964/fooling-the-smart-city/).

Eine kürzlich erschienene Studie der IT-Sicherheitsfirma Kaspersky zeigt, wie einfach sich Hacker in die Systeme der Verkehrskontrolle einhacken können und damit vollen Zugriff auf die Verkehrsinfrastruktur einer Stadt erlangen. Die Forscher konnten zum Beispiel ganze Kameranetzwerke anzapfen, da diese nicht passwortgeschützt waren. Dadurch ließ sich das Konfigurationsmenü von Blitzern umprogrammieren (vgl. https://www.welt.de/wirtschaft/webwelt/article158584087/Hacker-koennen-Tempo-Blitzer-problemlos-umprogrammieren.html). Kriminellen scheinen Tür und Tor geöffnet, da selbst einfachste Sicherheitsvorkehrungen zum Schutz vor unerlaubtem Zugriff vernachlässigt werden. Die Kaspersky Forscher kritisieren, wie ungeschützt viele Geräte der städtischen Verwaltung sind und wie einfach es Dritten gemacht wird, solche Systeme anzugreifen.

Datum des Originals: 15.11.2016/Ausgegeben: 18.11.2016

Solche Sicherheitslücken erobern zunehmend den Straßenverkehr. In einem Artikel vom 09.10.2016 berichtet die Bild von einem IT-Spezialisten, der sich in Ampelschaltungen einhacken und sie umprogrammieren konnte (http://www.bild.de/bild-plus/news/inland/informatiker/ampel-hacker-48199308,view=conversionToLogin.bild.html). Seiner Meinung nach sind „deutsche Ampeln eine leichte Beute für Hacker“. Zwei weitere IT-Spezialisten vom Security-Portal internetwache.org, bestätigten zuvor solche Sicherheitslücken in Ampelschaltungen in einem Computer Bild Artikel vom 29.09.2016 (http://www.computerbild.de/artikel/cb-News-Sicherheit-Jetzt-lassen-sich-auch-Ampeln-hacken-16414705.html). Ihnen ist es gelungen, über eine schon seit Jahren bekannte Sicherheitslücke Baustellenampeln zu kontrollieren und somit nach Belieben umzuprogrammieren. Diese beunruhigenden Beispiele zeigen, dass der digitale Schutz der Verkehrsinfrastruktur hohe Priorität genießen muss. Für einen grundlegenden Schutz sind nicht einmal große Investitionen nötig. Die einfachsten Maßnahmen wie passwortgeschützte Zugänge zu sensiblen Datenbanken, ein allgemeines und umfassendes Sicherheitsaudit, Sensibilisierung von Mitarbeitern, die für die Installation und Wartung von Überwachungssystemen zuständig sind, und die Einschränkung von externen Zugriffen aus dem Internet können bereits zu einer erhöhten Sicherung dieser Netzwerke beitragen.

Der Minister für Bauen, Wohnen, Stadtentwicklung und Verkehr hat die Kleine Anfrage 5245 mit Schreiben vom 15. November 2016 namens der Landesregierung im Einvernehmen mit dem Minister für Inneres und Kommunales beantwortet.

1. Sind der Landesregierung Manipulationen im Zusammenhang mit der Verkehrsinfrastruktur von Städten oder dem Land bekannt? (wenn ja, bitte auflisten!)

Die telematische Verkehrsinfrastruktur an Bundesautobahnen wird von der Verkehrszentrale NRW betrieben. Die Verkehrszentrale NRW hat bislang keine Fälle von Manipulationen an der Verkehrsinfrastruktur, die in ihrem Zuständigkeitsbereich liegen, verzeichnet. Die technischen Systeme der Verkehrszentrale NRW sind durch eine hochverfügbare Firewall geschützt, die aktuell auf den Stand der Technik gebracht wurde und rund um die Uhr überwacht wird.

Für die verkehrstechnische Infrastruktur in den Städten hat eine Anfrage an die zuständigen Fachvertretern im Deutschen Städtetag ergeben, dass Fälle von Manipulationen an kommunalen Lichtsignalanlagen nicht bekannt sind. Probleme werden auch von den im Artikel benannten Städten dementiert. In Bezug auf fest installierte Lichtsignalanalgen (LSA) werden die Sicherheitsfunktionalitäten in Deutschland gemäß DIN EN 50556 VDE 0832-100:2011-09 eigensicher aufgebaut und können nach Experteneinschätzung auf keinen Fall – nicht einmal durch die Systementwickler selbst - aus der Ferne manipuliert werden (safety by design).

2. Können falsche Geschwindigkeitsmessungen durch Manipulation von Radaranlagen entstehen?

Das Gesetz über das Inverkehrbringen und die Bereitstellung von Messgeräten auf dem Markt, ihre Verwendung und Eichung (Mess- und Eichgesetz - MessEG) sowie die gleichlautende Mess- und Eichverordnung (MessEV) beschreiben, dass Messgeräte, die der amtlichen Überwachung des öffentlichen Verkehrs dienen, zugelassen und geeicht sein müssen. Die Physikalisch-Technische Bundesanstalt in Braunschweig und Berlin (PTB) ist gemäß § 14 Abs. 3 MessEG für die Zulassung von Messgeräten zuständig. Vor Erteilen der Zulassung prüft die PTB die Plausibilität des Messprinzips und die korrekte Erstellung des Messwertes. Gleiches gilt für die Messwertbildung, die digitale Datensicherheit, die Gebrauchsanweisung und die

Darstellungssoftware. Die innerstaatliche Bauartzulassung oder die neue Baumusterprüfbescheinigung der PTB ist vergleichbar mit der Bauartzulassung des Kraftfahrtbundesamtes eines neu entwickelten Kraftfahrzeugs. Die Bauartzulassung verpflichtet das Messpersonal, das Messgerät nur nach den Vorgaben der Gebrauchsanweisung zu betreiben.
Nach einer Messung werden im Messgerät Messfoto und Messdaten nach den Vorgaben der PTB zu einem Datensatz zusammenführt, verschlüsselt, signiert und auf einem Datenträger gespeichert. Das Öffnen der verschlüsselten Messdaten ist nur über eine zugelassene Software möglich.
Die verwendeten Messgeräte bilden technisch ein abgeschlossenes System. Betrieb und Sicherung der Daten erfolgen nach den Standards des Bundesamtes für Sicherheit in der Informationstechnik (BSI-Standard).

3. Welche Maßnahmen hat die Landesregierung in ihrer Legislaturperiode ergriffen, um dieser Entwicklung entgegenzuwirken und mögliche Sicherheitslücken zu schließen?

Zukünftige moderne Messanlagen steuern die Messkomponenten und die Übermittlung des Messfotos über eine Funk-/WLAN-Datenverbindung. Die Steuerung der Messanlage und der Versand von Messdaten erfolgen verschlüsselt. Auch hier ist der BSI-Standard für die Art und Weise der Verschlüsselung vorgeschrieben und von der PTB in der Bauartzulassung geprüft.
Bei der Erstellung einer Leistungsbeschreibung für ein künftiges Ausschreibungsverfahren von Geschwindigkeitsmessanlagen ist eine Schutzbedarfsfeststellung erfolgt.
Die polizeilichen Geschwindigkeitsmessgeräte werden jährlich durch die örtlich zuständige Eichdirektion geeicht. Nicht geeichtes Messgerät oder ein Messgerät mit beschädigter Eichmarke darf nicht benutzt werden.

4. Sind Maßnahmen wie ein vollständiges Sicherheitsaudit zum Schutz von Geschwindigkeitsüberwachungskameras oder von Ampelschaltungen geplant bzw. bereits im Einsatz?

Der Schutz von Geschwindigkeitsüberwachungskameras unterliegt den Anforderungen des BSI. Der IT-Grundschutz gemäß BSI-Standards stellt inzwischen einen Quasi-Standard für Informationssicherheit dar.
Für die Vergabe eines ISO 27001-Zertifikats auf der Basis des IT-Grundschutzes wäre die Durchführung eines Audits durch einen externen, beim BSI zertifizierten Auditor vorgesehen.

Gemäß Auskunft des Deutschen Städtetags ist die Problematik in den damit befassten Fachkreisen der Kommunen bekannt und wird bearbeitet. Die Deutsche Kommission Elektrotechnik Elektronik Informationstechnik im DIN und VDE (DKE) hat einen Arbeitskreis „Schutzmaßnahmen gegen nicht autorisierte Zugriffe“ gegründet, der sich damit auseinandersetzt. Die geplante Version 3 des in vielen Städten im Einsatz befindlichen offenen Schnittstellenstandards für Verkehrsrechnersysteme und Lichtsignalanlagen wird z.B. eine Reihe von Maßnahmen zur IT-Sicherheit aufweisen. Verschiedene Städte haben seit etwa zehn Jahren ein Versionsmanagement auf dem Verkehrsrechner eingeführt, welches die Datenkonsistenz aller Lichtsignalanlagen online überwacht und bei Abweichungen Alarm schlägt. Ein nur zu regelmäßigen Auditterminen durchzuführendes Sicherheitsaudit wäre dagegen nicht geeignet, sicherheitsrelevante Fehler kurzfristig aufzudecken.

5. Verfügt die Landesregierung über Notfallpläne für Szenarien, in denen Hacker die Verkehrsinfrastruktur einer Stadt angreifen und somit Ordnung und Orientierung gefährden?

Nach Auskunft des Deutschen Städtetags existieren solche Pläne in den Städten nicht ausschließlich bezogen auf Lichtsignalanlagen oder Verkehrsinfrastruktur, sondern allgemein für sogenannte „kritische Infrastruktur“, die im Not- und Krisenfall gesichert werden muss. Die in der Presse kursierenden Szenarien basieren nach Einschätzung des Deutschen Städtetags mehr auf Befürchtungen und Vermutungen als auf Fakten (anders als Beispiele etwa aus den USA). Nach den Ausführungen unter 1 und 4 werden sie vom Deutschen Städtetag für unwahrscheinlich gehalten. Aus den angeführten Medienberichten wird nicht deutlich, ob es sich ausschließlich um separate Baustellen(Funk-)Ampeln von privaten Betreibern handelt, die von Außenstehenden vorgeblich manipuliert wurden, und welcher Art die Manipulation gewesen sein soll (z.B. eine Veränderung der Grünintervalle oder auch feindliches „Grün“?). Der letztgenannte gefährliche Eingriff in den Straßenverkehr wäre zudem strafrechtlich relevant.