Kaspersky Lab

Sicherheitslücken bei Verkehrssensoren

[26.04.2016] Im Rahmen der Initiative Securing Smart Cities hat Kaspersky Lab die Verkehrssensoren in Moskau untersucht. Die Sensoren können laut dem Unternehmen zur Sicherheitslücke einer Smart City werden.

Damit in modernen Großstädten auch zu Stoßzeiten der Verkehr rollt, erfassen Sensoren, Kameras und smarte Verkehrsleitsysteme Art und Anzahl der Fahrzeuge sowie deren Geschwindigkeit. „Städte sind auf valide Daten über den Verkehrsfluss für dessen aktuelle Steuerung und die zukünftige Planung angewiesen“, erklärt Denis Legezo, Sicherheitsexperte des Unternehmens Kaspersky Lab. „Wir haben herausgefunden, dass Verkehrssensoren viel zu leicht manipuliert werden können. Ein Problem, das sofort behoben werden muss, damit die Planung und Umsetzung zukünftiger städtischer Infrastrukturmaßnahmen nicht beeinträchtigt wird.“ Kaspersky Lab hat laut eigenen Angaben in einem Feldversuch im Rahmen der Initiative Securing Smart Cities die Verkehrssensoren in Moskau genauer betrachtet und Sicherheitslücken festgestellt. Beispielsweise sei die Herstellerfirma der Sensoren leicht am Gehäuse ablesbar. Dieser Hinweis habe es den Experten von Kaspersky Lab ermöglicht, Informationen des Herstellers zur Steuerungssoftware sowie die technische Dokumentation für die Sensoren online zu finden. Zur Übernahme der Steuerung hätte eine einfache Bluetooth-Verbindung genügt, da kein zuverlässiger Authentifizierungsprozess implementiert war und das Passwort per Brute-Force-Angriff geknackt werden konnte. Die technische Dokumentation des Herstellers habe außerdem genug Informationen geliefert, um die Geräte so zu manipulieren, dass in der Folge alle erfassten Daten zu Art und Geschwindigkeit der Fahrzeuge hätten verfälscht werden können. Deshalb empfiehlt Kaspersky Lab zum Schutz vor Manipulation nicht nur, die Kennzeichnung von den Geräten zu entfernen, sondern auch den Standardnamen der Geräte abzuändern und die Media-Access-Control (MAC)-Adressen der Hersteller nach Möglichkeit zu verdecken. Für die Bluetooth-Verbindung sollten eine zweistufige Authentifizierung und sichere Passwörter verwendet werden. Nicht zuletzt empfehle es sich, die Geräte von Sicherheitsexperten auf weitere Schwachstellen untersuchen zu lassen. Sollten Kriminelle Zugang zur Verkehrsinfrastruktur einer Smart City erlangen, könnten laut Kaspersky Lab nicht nur die über die Straßensensoren erfassten Daten manipuliert und kritische Daten modifiziert, verfälscht oder gelöscht werden. Auch bestehe die Gefahr, dass teure Smart-City-Ausrüstung zerstört oder die Arbeit der zuständigen Stadtbehörde sabotiert werde.

(ve)

Stichwörter: IT-Sicherheit, Smart City, Kaspersky Lab