CyOne Security AG
Hinterbergstrasse 18
6312 Steinhausen

Telefon +41 41 748 85 00
info@cyone.ch
cyone.ch

WISSENS-UPDATE

IoT-Sicherheit im Fokus – damit die Smart City nicht zur Risikozone wird

Städte werden vernetzter und intelligenter. Das ist grundsätzlich zu begrüssen. Das Problem: Die Smart City nimmt so schnell Form an, dass Verantwortliche aus der Verwaltung und Lieferanten aus der Industrie zu oft ausschliesslich auf die entsprechenden Funktionali-täten fokussiert sind. Der dafür notwendigen Cyber-Sicherheit wird kaum nachgekommen. Der soziale, ökologische oder ökonomische Mehrwert für die Menschen der Smart City kann dadurch schnell zum Fiasko werden.

Die Vision der Smart City klingt verlockend. Intelligente Technologien sollen unsere Städte lebens-werter machen. Die kluge Vernetzung von Bereichen wie Umwelt, Energie und Verkehr ermöglicht eine effizientere Nutzung der urbanen Infrastruktur – so das Versprechen der Smart City. Die Bevölkerung soll auf verschiedensten Ebenen profitieren: weniger Stau, keine Parkplatzsuche mehr, effizientere Verbindungen im öffentlichen Verkehr, bessere Luftqualität, höhere Energieeffizienz und bequemere Services in der Verwaltung.

Städte rund um die Welt stürzen sich voller Enthusiasmus in die Umsetzung dieser Vision. Ein Vorzeigebeispiel ist Barcelona: Die Stadt ist bereits hochgradig mit Sensoren vernetzt und die intelligente Datenanalyse steigert die Effizienz der städtischen Infrastruktur – von der Parkplatz-bewirtschaftung über die Müllabfuhr bis hin zur Bewässerung von Grünanlagen.

IT-Sicherheit wird vernachlässigt

In der Euphorie über das enorme Potenzial der Vernetzung, wird in den Städten in den meisten Fällen nur dem Thema «Schutz von Personendaten» eine gewisse Bedeutung beigemessen. Dies

vermutlich hauptsächlich, um die verantwortlichen Datenschützer nicht auf den Plan zu rufen. Die eigentlichen Risiken dieser Vernetzung von Mensch, Organisation und Infrastruktur werden in den allermeisten Fällen aber oft vergessen. So werden etwa smarte Verkehrsampeln und Strassenlampen installiert, ohne über das mögliche Schadenspotenzial der Technologie und die Auswirkungen bei einer möglichen Manipulation durch Cyber-Kriminelle nachzudenken. Da werden sorglos städtische Wasser-Sprinkleranlagen in Parks, Bodenhydrometer, Temperatursensoren mit städtischen Wasserspeicher-Werken vernetzt, welche anhand von Wetterprognosen eine optimale Bewässerung sicherstellen sollen. Eine mögliche Auswirkung auf die Trinkwasserversorgung der Bevölkerung durch eine Übernahme des Speicherwerkes von Cyber-Kriminellen ist kein Thema.

Cyber Security-Experten sind sich einig: IT-Sicherheit wird von den meisten Smart Cities sträflich vernachlässigt. Zwar testen die Städte die Systeme auf ihre korrekte Funktionalität. Danach stehen aber andere Faktoren wie Wetterfestigkeit im Fokus. Die potenzielle Verwundbarkeit durch mögliche Cyber-Attacken infolge der Vernetzung verschiedener Infrastrukturen von unterschiedlicher gesellschaftlicher Wichtigkeit steht heute noch viel zu wenig im Vordergrund. Den meisten Stadtverwaltungen wie auch den Anbietern der smarten Lösungen fehlt die Expertise im Umgang mit Cyber Security.

Dabei haben Cyber-Attacken das Schadenspotenzial vernetzter Technologien in der Vergangenheit bereits mehr als deutlich gemacht: 2015 haben Cyber-Kriminelle die Stromversorgung von Kiew lahmgelegt. 2016 fielen in San Francisco einen Tag lang alle Fahrkartenautomaten aus. 2017 lösten Hacker in Dallas auf über 150 Sirenen einen Fehlalarm aus, der die Bevölkerung in Angst und Schrecken versetzte. 2018 wurde das städtische IT-System von Atlanta mit Schadsoftware infiziert, worauf es zu Ausfällen in der Stadtverwaltung kam.

Fatale Sicherheitslücken

Diese Beispiele zeigen es: Smart Cities sind auf vielen Ebenen verwundbar – sei es im Verkehr, der Verwaltung oder der Energie- und Wasserversorgung. Das schwächste Glied der Systemkette ist dabei oftmals Ausgangspunkt für Cyber-Attacken. Bezahlterminals, Parkleitsysteme, Fahrradmietsysteme oder sogar vernetzte Temperatursensoren sind alles potenzielle Einfallstore. Die Drahtlosverbindungen, mit denen die Systeme untereinander kommunizieren, sind häufig unzureichend zugangsgesichert, und auf eine Verschlüsselung der Kommunikation wird vielfach verzichtet. Zudem sind die Übergänge von unkritischen Systemen (z.B. Fahrzeugzählsensor) zu den kritischen Systemen des Eco-Systems (z.B. Verkehrsampel) ungenügend geschützt bzw. werden nicht überwacht.

X-Force Red, die Sicherheitsabteilung von IBM, hat Smart City-Lösungen verschiedenster Anbieter getestet und dabei zahlreiche Sicherheitslücken aufgedeckt. Viele der Geräte sind nur durch Standardpasswörter geschützt. In einigen Fällen war es gar möglich, sich ohne gültige Zugangsdaten anzumelden. Zudem sind manche Systeme prädestiniert für sogenannte SQL-Injektionen.

Grosser Handlungsbedarf: IoT-Sicherheit

All diese Sicherheitslücken sind typisch für das Internet of Things (IoT). In den letzten Jahren wurden Millionen kaum geschützter Geräte mit dem Internet verbunden – eine Armada von Druckern, Kameras und Routern, die Hacker bereits für unterschiedlichste Zwecke ausgenutzt haben. IoT-Technologien sind auch in der Smart City zentral. Die Verwendung im sicherheitssensitiven Kontext der Grossstadt macht eine stärkere Regulierung der IT-Sicherheit bei IoT-Geräten umso dringlicher. Anbieter müssen Sicherheitsfragen ernster nehmen.

Handlungsbedarf gibt es auch in den Stadtverwaltungen. Sie müssen einerseits die notwendigen Sicherheitsmerkmale bei den Anbietern konsequent einfordern und andererseits ihre Kompetenzen im Bereich der Cyber Security ebenfalls ausbauen. Dabei ist eine Zusammenarbeit mit Spezialisten unumgänglich. Vor der Implementierung smarter Technologien sind diese eingehend auf Cyber-Risiken zu überprüfen. Mit der fortschreitenden Vernetzung gilt es, die Infrastruktur zudem regelmässig und systematisch auf Schwachstellen hin zu überprüfen. Dabei ist den Übergängen zu kritisch eingestuften Infrastrukturen besondere Aufmerksamkeit zu schenken. Nur wenn die IT-Sicherheit künftig oberste Priorität hat, wird die Smart City auch sicher sein und sozial, ökologisch und ökonomisch den Mehrwert für die Menschen erbringen.

CyOne Security ist der kompetente Partner

Bei der Entwicklung von Smart Cities bleibt, wie oben beschrieben, die Sicherheit oft auf der Strecke, weshalb bisherige Sicherheitsansätze grundlegend überdacht werden müssen. Verfügbarkeit, Verhinderung von Zweckentfremdung und Wahrung der Datensicherheit sind zwingende Voraussetzungen für eine seriöse Nutzung des enormen Potenzials, das die neuen digitalen Welten für uns bereithalten.

Informations- und Datensicherheit ist ein substanzieller Bestandteil in der Entwicklung von Smart Cities. Um die vernetzten Produkte und Systeme vor Cyber-Attacken zu schützen, bringt die CyOne Security tiefes Expertenwissen in Cipher- und Cyber-Security in die Sicherheitskonzepte und -lösungen ein, die auf der 360°-Sicherheitskompetenz von Product Security, System Security und Operational Security basieren.

Beginnen Sie heute und schützen Sie die vernetzen Dinge in der Smart City vor Cyber-Risiken.

Machen Sie den ersten Schritt: Analysieren Sie gemeinsam mit unseren Experten Ihre aktuellen und zukünftigen Sicherheitsbedürfnisse Ihrer vernetzten Produkte, damit wir mit Ihnen über zielgerichtete Sicherheitslösungen diskutieren können.

Kontaktieren Sie uns für ein kostenloses Expertengespräch.