Smart City wird zum Trend in den Kommunen. Tenable erklärt, warum die IT-Sicherheit hierbei nicht vergessen werden darf.

Sicherheit in der „Smart City“ – worauf es ankommt

Technologien verändern unseren Alltag, das zeigt ein kurzer Blick auf die Kommunikation: Vom Anruf per Festnetztelefon, hin zu WhatsApp, Mail und vielen anderen Möglichkeiten. Dieser Wandel geht noch weiter: Smarte Geräte sind Standard und nicht nur unsere Telefone und Tablets, auch Fernseher, Kühlschränke und Heizungen kommunizieren mittlerweile über das Internet miteinander und mit uns. Die Vernetzung macht jedoch heute nicht mehr an der Haustüre halt: Viele Kommunen setzen auf die „Smart City“, um den Verkehr effizient zu regeln oder das Parken besser zu organisieren. Tenable erläutert, warum der Faktor Sicherheit bei Smart Cities oft vergessen wird und worauf es für Städte ankommt.

Mit größerer Vernetzung entstehen neue Angriffsflächen für Hacker
Je smarter die Welt, desto mehr Angriffe auf Infrastrukturen und Geräte. In Zukunft gilt das auch für die kommenden Smart Cities. Dass diese gewünscht sind, ist eindeutig: 91 Prozent der Befragten gaben in der Studie „Digitale Stadt“ des Branchenverbands Bitkom an, dass sie sich ein Parkplatzleitsystem wünschen, 94 Prozent würden sich über eine intelligente Verkehrssteuerung zur Staureduzierung freuen. Deutsche Städte wie Duisburg gehen bereits voran und bauen ihre Infrastruktur dem technologischen Fortschritt entsprechend aus. In naher Zukunft soll hier alles smart sein: der Bildungsbereich, Straßenlaternen, Verkehrsmanagement und Verwaltung. Andere Städte wie z.B. Talinn (Estland) testeten schon 2017 autonomen ÖPNV. Die Digitalisierung von gesamten Infrastrukturen ist also nur noch eine Frage der Zeit. Doch wie steht es um die Sicherheit?

Smarte Infrastrukturen machen neue Sicherheitsansätze notwendig
Bieten die bekannten Methoden die nötigen Einblicke und ausreichendes Wissen, um diese erweiterten Umgebungen wirkungsvoll zu schützen? Das ist nicht der Fall. Nötig ist ein neuer, umfassender Ansatz, der die gesamte Angriffsfläche erkennt. Um diese neuen Herausforderungen in den erweiterten, modernen Umgebungen zu beschreiben, hat sich der Begriff Cyber Exposure etabliert. Cyber Exposure fokussiert darauf, wo Schwachstellen bestehen und wie diese reduziert werden können. Das Wissen über die Cyber Exposure ist entscheidend, um die Gefahren vollständig zu verstehen, damit Verantwortliche die richtigen, sicherheitsrelevanten Entscheidungen treffen können – schließlich steht einiges auf dem Spiel, vor allem wenn es um öffentliche Infrastrukturen vernetzter Städte geht.

Kontinuierliches Monitoring, um Cyberrisiken zu erkennen und zu verringern
Höchste Priorität hat es, sämtliche im Netzwerk eingebundene Assets zu identifizieren und möglichst durchgängig zu scannen, um alle Schwachstellen zu finden. Für dieses kontinuierliche Monitoring plädiert auch das BSI. Verantwortliche sollten Cyber-Exposure-Lösungen nutzen, um sich vollständig abzusichern. Erst sie geben umfassenden Einblick in alle Assets, von IT, Cloud und IoT (Internet of Things) bis hin zu OT (Operational Technology). Anschließend nutzen die Lösungen dieses Wissen über die

Schwachstellen und erstellen darauf basierend eine Liste der Probleme, die anhand des geschäftlichen Risikos priorisiert werden. Erst mit diesem Bezug auf die tatsächlichen Gefahren für den Geschäftsbetrieb haben Sicherheitsbeauftragte die nötigen Daten zur Hand, um relevante Entscheidungen zu treffen: Wo sind die Schwachstellen? Mit welchen Maßnahmen und Technologien senken sie diese Sicherheitsrisiken? Der umfassende Einblick und die Priorisierung der Probleme durch Cyber-Exposure-Lösungen kann diese Informationen bieten.

Seien wir ehrlich: Smart Cities sind aufgrund des technologischen Fortschritts bald Realität – es geht darum, wie sicher die Verantwortlichen sie gestalten. Dafür ist Aufmerksamkeit für das Thema Sicherheit nötig: Städte dürfen das Thema Security nicht aus den Augen lassen. Ein guter Schutz verhindert Vorfälle und stärkt das Vertrauen der Bürgerinnen und Bürger in die Smart City – sodass diese am Ende so akzeptiert sind, wie Mail, WhatsApp oder Festnetztelefon.

Bei Fragen melden Sie sich bitte!

Duygu Duru
Account Manager
HBI Helga Bailey GmbH - International PR & MarCom
Stefan-George-Ring 2 **|** 81929 München

T: +49 (0) 89 99 38 87 44 **| M:** +49 (0) 174 31 02 959
Duygu_Duru@hbi.de **|** www.hbi.de