MEINUNGEN

WERDEN WIR DIE SMART CITY MORGEN WIRKLICH SCHÜTZEN KÖNNEN?

Vincent Nicaise
Manager für Industriepartnerschaften und das Ökosystem der Industrie bei Stormshield

Die Stadt von morgen verspricht, Online-Vorgänge zu erleichtern, den Verkehr flüssiger zu gestalten und den Energieverbrauch zu optimieren. Aber jeder neue digitale Dienst ist auch eine weitere Gelegenheit für einen Cyberkriminellen, die Kontrolle zu übernehmen oder die gesammelten Daten abzuschöpfen. Welche Cyberrisiken und Schutzmaßnahmen gibt es also für die Smart City?

Durch das Angebot von immer mehr digitalisierten Diensten werden Smart Cities immer vernetzter... aber auch anfälliger für Cyberrisiken. Die Nachrichten sind voll von Beispielen **lokaler Behörden, die Opfer von Ransomware wurden**, mit dem Schreckgespenst, dass einige oder alle ihre Dienste lahmgelegt wurden. Mehr denn je ist Cybersicherheit ein vorrangiges Thema für Gemeinden, und noch mehr für vernetzte Städte.

LOKALE BEHÖRDEN IM VISIER VON CYBERATTACKEN

Frankfurt in Deutschland, New York in den Vereinigten Staaten, La Rochelle und Angers in Frankreich, und zuletzt Lüttich in Belgien ... in den letzten Monaten sieht die Liste der Städte, die von einem Cyberangriff betroffen waren, wie eine Aufzählung ohne Ende aus. Seit dem öffentlichkeitswirksamen Präzedenzfall, bei dem die Stadt Baltimore, USA, 2019 Opfer einer Ransomware-Attacke wurde, die Berichten zufolge 18 Millionen Dollar kostete, verschärft sich das Phänomen. So sehr, dass heute die Aktivitäten jeder Gemeinschaft verlangsamt, blockiert... oder verändert werden können.

Im Jahr 2019 wurden mehr als 1.200 französische Kommunen Opfer von Cyberangriffen. Eine Zahl, die laut dem Aktivitätsbericht des Jahres 2020 der Plattform Cybermalveillance.gouv.fr im Jahr 2020 um 72 % gestiegen ist. „*Lokale Behörden verfügen über Daten, die für Hacker sehr wertvoll sind, wie zum Beispiel Personenstandsdaten*“, erklärt **Jérôme Notin**, Generaldirektor von Cybermalveillance.gouv.fr, in einem Interview mit Journal du net. „*Das Geburtsdatum, der Geburtsort und die Adresse einer Person können verwendet werden, um falsche Dokumente zu erstellen oder sich Zugang zu den Online-Konten anderer Opfer zu verschaffen, die durch geheime Fragen nach diesen Informationen gesichert werden können.*“ Dies veranlasste die ANSSI im vergangenen Jahr, einen Leitfaden (in französischer Sprache) zur Sensibilisierung von Unternehmen und lokalen Behörden für dieses Thema zu veröffentlichen. Aber die Bedrohung ist nicht vorbei und **Smart Cities stellen eine neue Chance für Angreifer dar.**

SIND VERNETZTE STÄDTE VERWUNDBARE STÄDTE?

Smart City ist ein Oberbegriff, der verschiedene Domänen und unterschiedliche Akteure zusammenfasst. Das Ziel ist es, die großen Herausforderungen der Städte von morgen (Energiewende, galoppierende Demografie, Ressourcenmanagement, Gesundheit usw.) zu bewältigen, indem man sich auf neue Technologien stützt, wie **Jocelyn Zindy**, Cybersicherheit Sales Director, und **Grégory Coustou**, Chief Technology Officer bei Eiffage Energie Systèmes, ausführlich beschreiben. „*Auf der physischen Ebene werden in der Smart City Sensoren eingesetzt, um die Müllabfuhr zu optimieren, Überschwemmungen zu erkennen, Parkplätze oder Fahrzeugladestationen zu verwalten. Überwachungskameras sind ein weiterer wertvoller Verbündeter in dieser städtischen Umgebung. Sie wurden ursprünglich für die Videoüberwachung eingesetzt, aber ihre Anwendungsmöglichkeiten haben sich vervielfacht: Lesen von Nummernschildern, Analyse des menschlichen Verhaltens, Gefahrenanalyse, Erkennung von isolierten Objekten, dynamische Verwaltung der Straßenbelegung, Informationsquelle für autonome Shuttles. Und auf der anderen Seite, auf der digitalen Ebene, ermöglichen es die neuen Edge-Computing-Architekturen, alle Daten so nah wie möglich am Ort ihrer Entstehung zu verarbeiten und Technologien der künstlichen Intelligenz wie maschinelles Lernen zu nutzen. Dies bedeutet einen Gewinn bei der Dimensionierung zentraler Infrastrukturen und auch bei der Wartung. Schließlich ermöglichen IT-Plattformen die zentrale Verwaltung dieser miteinander verbundenen Systeme und unterstützen die Straßenarbeiter bei den Wartungsarbeiten.*“

Diese vernetzten Städte sind also eine Konvergenzzone unterschiedlicher Informationssysteme verschiedenster Akteure, mit unterschiedlichen technologischen Bausteinen (5G, IoT, Edge, KI), unterschiedlicher Ausstattung (Stadtmobiliar, Ampeln, öffentliche Beleuchtung, Sensoren usw.) und unterschiedlichen Schnittstellen (mobile Anwendungen, Datenaustausch zwischen IS wie dem Lehren von Bürgerpflichten), **die die Angriffsfläche einer Smart City erheblich erweitern**. Anders ausgedrückt: Die Smart City akkumuliert Heterogenitäten.

Heterogene Geräte

Die Smart City muss sich auf ihre bestehende Flotte verlassen. Das bedeutet, dass man es mit verschiedenen Generationen von Anlagen und unterschiedlichen Technologien zu tun hat, was die Umsetzung einer globalen Sicherheitspolitik erschwert. „*Wir müssen sowohl die technischen Maßnahmen, also die zu implementierenden Sicherheitslösungen, als auch die organisatorischen Maßnahmen an den Kontext, das Informationssystem, die Gerätegeneration und die verwendeten technologischen Bausteine anpassen*“, betont **Khobeib Ben Boubaker**, Leiter der Sparte Industrial Security bei Stormshield.

Anlagen, die oft gefährdet sind, weil sie sich in der Stadt befinden, für alle sichtbar und daher leichter zugänglich sind: Ampeln, Wasser-, Gas- und Stromnetze usw. „*Bei einem traditionellen Büroinformationssystem weiß man, dass der Serverraum an diesem und jenem Ort ist, dass er durch einen Ausweis gesichert ist und dass man keinen Zugang dazu hat*“, fährt Khobeib Ben Boubaker fort. *In Smart-City-Umgebungen ist der Zugriff auf Geräte recht einfach. Die Zugänglichkeit zu den Geräten und die Sicherheit sind daher wichtige Themen.*“

Heterogene Ziele

Die Smart City vereint unabhängige Informationssysteme, die miteinander vernetzt werden müssen. An dieser Stelle wird es kompliziert, wenn es um Cybersicherheit geht. „*Wir müssen eine globale Sicherheitspolitik aufstellen und sie dann an jedes einzelnes IS anpassen*“, betont Khobeib Ben Boubaker.

Darüber hinaus umfasst die Smart City mehrere Netzwerkperimeter: IT und OT. Aber diese haben nicht die gleichen Probleme. „*Für die IT ist das Hauptproblem die Vertraulichkeit der Daten. Und im OT geht es darum, dass der Dienst kontinuierlich verfügbar ist. Die Prioritäten sind nicht dieselben, also werden die zu implementierenden Sicherheitsregeln anders sein*“, argumentiert Khobeib Ben Boubaker. „*Dies impliziert eine globale Governance, die an jedes Subsystem angepasst ist.*“ Ein zentrales Thema der Fragen der Cybersicherheit in der Industrie.

Heterogene Akteure

Allein beim Thema Mobilität gibt es beispielsweise einen Mix aus traditionellen Akteuren, Anbietern von sanfter Mobilität (Roller oder Fahrräder), Anbietern von Software- oder Cloud-Lösungen und staatlichen Diensten. Unter diesen Bedingungen ist es schwierig, sich auf einen globalen Ansatz zu einigen.

„In der Smart City kann man Cybersicherheit nicht überall auf die gleiche Weise umsetzen. Sie müssen verstehen, wie das System funktioniert und was auf dem Spiel steht, um zu bestimmen, was kritisch ist und was nicht. Dazu muss man in der Lage sein, sowohl mit den Geschäfts- als auch mit den Cybersicherheitsleuten zusammenzuarbeiten", warnt Khobeib Ben Boubaker.

Heterogene Referenzsysteme

Diese Pluralität der Akteure führt zu einem Wirrwarr von Referenzsystemen. „*Was wir von Projekt zu Projekt feststellen, ist, dass es keine Harmonie gibt: Einmal wird diese Kommunikationstopologie oder diese Technologie verwendet, ein anderes Mal eine andere*", bemerkt Khobeib Ben Boubaker. „*Manchmal ist es gut dokumentiert und wir können das richtige Maß an Sicherheit bieten. In anderen Fällen ist sie nicht genormt. Die erste Aufgabe der Smart City ist daher die Harmonisierung der Referenzsysteme.*"

Es liegt also im Interesse der Städte, wachsam zu sein... und das Kleingedruckte zu lesen! „*Die Analyse von Vertragsklauseln in aktuellen und zukünftigen Verträgen ist eine Priorität,*" stellt der von der AMF veröffentlichte Cybersicherheit Guide im November 2020 fest. „*Es ist zwingend erforderlich, in Dienstleistungs- oder Subunternehmerverträgen zu identifizieren, wo die Lücken oder Schwachstellen in der digitalen Sicherheit liegen könnten. Es ist nicht ungewöhnlich, dass Vertragsklauseln den Sicherheitszielen der Gemeinschaft zuwiderlaufen oder dass es einfach keine Klauseln gibt, die eine gute Sicherheit garantieren (Zeit bis zur Rückkehr zum Normalzustand, Sicherung/Wiederherstellung, Reversibilität usw).*"

Wenn die Stadt die delegierte Verwaltung einsetzt, ist es besser, in den Spezifikationen die Bedingungen für die Verwaltung des Informationssystems im Allgemeinen (und der personenbezogenen Daten im Besonderen) zu definieren.

Heterogene Normen

In Bezug auf die Einhaltung von Vorschriften muss die Smart City verschiedene Normen und Vorschriften sowohl auf europäischer als auch auf nationaler Ebene integrieren. Dazu gehören die DSGVO für personenbezogene Daten und die NIS-Richtlinie für bestimmte Dimensionen im Zusammenhang mit KRITIS-Betreibern (kritischen Infrastrukturen) oder das Militärprogrammierungsgesetz in Frankreich für Betreiber von entscheidender Bedeutung (OIV) zu Themen wie Energie, Wasser, Abfallwirtschaft, Gesundheit, Transport usw.

Was die Frage der Verantwortung angeht, so wird sie geteilt. Die Delegation der Verwaltung einer Kompetenz bedeutet keine Übertragung der Verantwortung. *„Der Delegierende und der Delegierte sind gemeinsam für die allgemeine Sicherheit verantwortlich. Die Vereinbarung sollte explizite und ausdrückliche Klauseln enthalten, die die Aufteilung der Verantwortlichkeiten und Pflichten zwischen den beiden Partnern festlegen*," empfiehlt die AMF.

Zumal die vernetzten Dienste von Städten sensible Elemente betreffen können, wie z.B. Energienetze (Strom, Gas, Wasser) oder Krankenhäuser. In jedem Fall muss die Stadt darauf achten, Mustervertragsklauseln zu definieren, die in ihre zukünftigen Verträge aufgenommen werden sollen, und sich bei deren Ausarbeitung rechtlich und technisch beraten lassen.

INTEGRATION DER SICHERHEIT IN DAS DESIGN VON SMART CITIES

Je intelligenter und vernetzter Städte werden, desto mehr sind sie Cyberbedrohungen ausgesetzt - mit sehr realen Folgen für die Bürger. *„Wenn wir die Sicherheit nicht von der Designphase an integrieren, kann es zu echten Dramen mit physischen Folgen kommen*", betont Jérôme Notin im Journal du Net. *„Zum Beispiel, wenn wir rote Ampeln blockieren oder die vernetzten Glühbirnen der Stadt nutzen, um DDoS-Angriffe durchzuführen und andere Netzwerke zum Absturz zu bringen. Derzeit sind uns keine Fälle dieser Art in Frankreich bekannt. Auch die Hersteller dieser Systeme tragen eine gewisse Verantwortung, da sie nicht immer das Security-by-Design-Prinzip integrieren, um ihre Produkte schnell freizugeben*." Die Smart City wird durch die neuen Technologien mit neuen Schwachstellen konfrontiert. *„Das Datenmanagement ist heute ein strategischer Punkt in der Smart City, so wie es das Netzwerkmanagement vor 10 Jahren war*", betont Grégory Coustou.

„Die Cybersicherheit muss von Anfang an eingebettet und während des gesamten Projekts gelebt werden, um dem „Add-on"-Ansatz ein Ende zu machen, bei dem Schichten von Cybersicherheit hinzugefügt werden, um Verstöße im Nachhinein zu beheben"

Khobeib Ben Boubaker, Leiter der Sparte Industrial Security bei Stormshield

Die Cybersicherheit einer Smart City muss daher ihre Entwicklung im Laufe der Zeit antizipieren. Um dies zu erreichen, gibt es nur eine Methode: Die Cybersicherheit muss in jeder Phase, auch bereits in der Entwicklungsphase, eines Smart-City-Projekts berücksichtigt werden. *„Wenn das Projekt beginnt, muss man die Skalierbarkeit des IS berücksichtigen und an die Herausforderungen und Anwendungen von morgen denken. Die Cybersicherheit muss von Anfang an eingebettet und während des gesamten Projekts gelebt werden, um dem „Add-on"-Ansatz ein Ende zu machen, bei dem Schichten von Cybersicherheit hinzugefügt werden, um Verstöße im Nachhinein zu beheben*" beklagt Khobeib Ben Boubaker. *„Die Cybersicherheit ist ein Punkt der Wachsamkeit auf allen Ebenen und beginnt auf der Sensorebene*", ergänzt Jocelyn Zindy. *Die Wahl der Geräte ist daher von entscheidender Bedeutung, da die Sicherheit jedes einzelne kommunizierende Gerät, die Netzwerk- und Systeminfrastruktur, die Betriebszentren (Client-Arbeitsplätze, Handys, Tablets usw.) und auch die Benutzer (Gewohnheiten, Bewusstsein usw.) betrifft*.

DIE SMART CITY BRAUCHT MASSGESCHNEIDERTE CYBERSICHERHEIT

Einige Initiativen sind wegweisend. In Frankreich experimentiert die Stadtgemeinde Saint-Quentin-en-Yvelines mit einer Cybersicherheitslösung für ihre öffentliche Beleuchtung. Das Forschungsprojekt Paclido hat zum Ziel, die Sicherheit von vernetzten Objekten zu verbessern. Dabei geht es sowohl um den „physischen" Schutz der Anlagen als auch um die Sicherung des Datenaustauschs. *„Mit Paclido kann eine künstliche Intelligenz Cyberangriffe erkennen. Sie hat die normale Funktion der Beleuchtung gelernt und weiß, wie sie eine Anomalie erkennen kann*", erklärt **Guillaume Séraphine**, der Referent des Projekts, in *Smart City Mag. Die Kryptographie fügt eine zusätzliche Sicherheitsebene hinzu, indem sie die Daten verschlüsselt. Es ist wichtig, unser Internet der Dinge abzusichern, denn wenn es mit unserem Informationssystem verbunden ist, darf es morgen keinen Lücken haben*."

Die Cybersicherheit der Smart City ist ein langfristiges Thema mit einem sich ständig weiterentwickelnden Umfang. Diese vernetzten Städte benötigen daher einen speziellen Ansatz, der aus Folgendem besteht:

- **Installation verschiedener Sicherheitsstufen:** Datenverschlüsselung, Firewall, Authentifizierung, Zugriffsrechteverwaltung usw,
- **Einführung von hoheitlichen Lösungen,** die an hoheitliche Vorschriften angepasst sind, da es sich um öffentliche Lösungen des Staates handelt, um die technologische Autonomie zu gewährleisten, die umgesetzt wird,
- **Globale Cyber-Governance** mit der Implementierung eines SOC in der Stadt, das die Sicherheitsereignisse der verschiedenen IS verwaltet und feststellt, ob es keine Überläufe zwischen diesen Systemen gibt,

- **Segmentierung von Systemen:** Alle Informationssysteme sind miteinander verbunden. Daher ist es wichtig, sie zu partitionieren, um zu vermeiden, dass Korruption von einem System zum anderen überspringt. *„Manchmal ist der Einstiegspunkt nicht das Zielsystem, und die Verbreitung von vernetzten Objekten eröffnet noch mehr Einstiegspunkte, um auf ein kritisches System und Daten zuzugreifen*", warnt Khobeib Ben Boubaker,
- **Durchführung einer Kartierung der Geräte und des IS.** *„Wir können kein IS sichern, das wir nicht kennen. Wir müssen eine klare Vorstellung davon haben, was gesichert werden muss und welche Geräte hinzugefügt werden*", betont Khobeib Ben Boubaker,
- **Sicherstellung der Interoperabilität von Lösungen** zur Erhöhung des Sicherheitsniveaus,
- **Aufnahme von Cybersicherheits-Klauseln in städtische Verträge,** die die Aufteilung der Verantwortlichkeiten und Pflichten zwischen den Partnern festlegen,

Die Versprechen der Smart City sind zahlreich, sowohl in Bezug auf die Lebensqualität als auch auf den Umweltschutz. Diese Versprechen können ohne effektive Cybersicherheit nicht erfüllt werden.