Cyber Security für Smart Cities

REDGUARD
SECURING YOUR ASSETS

REDGUARD
SECURING YOUR ASSETS

Redguard AG
Eigerstrasse 60
CH-3007 Bern

Redguard AG
Josefstrasse 225
CH-8005 Zürich

Phone: +41 (0)31 511 37 50
E-Mail: contact@redguard.ch
www.redguard.ch

Die Entwicklung von Technologien verändert die Funktionsweise von Städten, bietet verbesserte Lebensbedingungen und effizientere Nutzungen von Ressourcen.

Gleichzeitig schaffen ICT-Trends, beispielsweise die Digitalisierung oder Internet of Things (IoT), neue Angriffsfläche für Hacker. Das Ziel der Angreifer ist, auf sensible Daten zuzugreifen, Systemausfälle zu erzeugen und geistiges Eigentum zu stehlen. Städte sind regelmässig mit Angriffen konfrontiert, und jeden Tag steigt der technischer Entwicklungsstand der Attacken.

Wer die Risiken kennt und seine ICT-Systeme richtig schützt, kann von den technischen Möglichkeiten profitieren und Datensicherheit sowie störungsfreie Systeme gewährleisten.

Der Smart-City-Experte ELEKTRON und die Experten für Informationssicherheit von Redguard haben sich mit Sicherheitsaspekten von Smart Cities auseinandergesetzt. Hier geben wir Ihnen einen Überblick über die wichtigsten Security-Themen.

Um eine Smart City sicher, verlässlich und gemäss geltenden Datenschutzbestimmungen zu gestalten, sollte sowohl die Infrastruktur wie auch Prozesse analysiert und zukunftsorientiert aufgesetzt sowie das Bewusstsein der Mitarbeitenden geschult werden.

REDGUARD
SECURING YOUR ASSETS

Die Redguard AG ist ein Schweizer Beratungsunternehmen für Informationssicherheit. Die unabhängige und neutrale Beratung umfasst organisatorische, technologische sowie menschliche Aspekte und beurteilt das Thema Informationssicherheit im Gesamtkontext.
www.redguard.ch

ELEKTRON
power on

Die ELEKTRON AG engagiert sich im Energie- und Infrastrukturmarkt durch Steigerung der Energieeffizienz. Als Smart-City-Systemintegrator begleitet ELEKTRON vernetzte Kommunikationsinfrastruktur rund um den digitalen Lichtpunkt.
www.elektron.ch

Komplexere IT-Systeme bringen zusätzliche Cyber-Bedrohungen

Eine Smart City besteht aus verschiedene Systemen, mit denen die Aktivitäten einer Stadt gesteuert, verwaltet und geplant werden. Dazu gehören beispielsweise die physische, soziale und wirtschaftliche Infrastruktur. Durch den technologischen Wandel werden IT-Systeme auf vielfältige Weise in allen Städten integriert, vom Gesundheitswesen und der Bildungsbranche bis hin zur Wasser- und Energieversorgung.

Dadurch wird auch die Informationssicherheit zu einem komplexeren Thema: internen IT-Systeme werden vernetzter und es werden mehr externe Partner an die IT-Systeme angebunden. Die Sicherheitsvorkehrungen müssen sich diesen neuen Anforderungen anpassen und alle Teilnehmer involvieren.

Mit der Entwicklung der Technologie halten auch die Kriminellen mit. Ihr Ziel ist, auf sensible Daten zuzugreifen, grösstmöglichen Schaden zu verursachen und wichtiges geistiges Eigentum zu stehlen. Städte sind regelmässig mit Angriffen konfrontiert, und jeden Tag steigt ihr technischer Entwicklungsstand. Die Art und der Umfang der Cyber-Bedrohungen ändern schnell – das potenzielle Ausmass der Probleme, mit denen Städte in Zukunft konfrontiert sein könnten, lässt sich heute kaum bestimmen. Eines ist aber sicher: Mit zunehmender Komplexität der Technologieintegration steigt auch das Risiko von erfolgreichen Cyber-Angriffen.

Die drei Bereiche der Informationssicherheit

Eine absolute Sicherheit vor Cyber-Angriffen gibt es nicht und alle Organisationen sind potenzielle Ziele. Das Risiko vor Angriffen können Sie jedoch drastisch senken, wenn Sie Informationssicherheit richtig angehen. Informationssicherheit – das ist die Umsetzung der Ziele Vertraulichkeit, Integrität und Verfügbarkeit für IT-Systeme und die darin gespeicherten oder verarbeiteten Daten.

Vertraulichkeit

Organisationen in Städten verfügen über sehr persönliche Daten ihrer Einwohner, beispielsweise Personendaten, AHV-Nummern, Strafauszüge, Zahlungsinformationen Steuerunterlagen oder Krankenakten. Dabei handelt es sich um vertrauliche Informationen, die von den Organisationen vertraulich behandelt werden müssen. Dieser Anstieg und die Zentralisierung von privaten Daten kann von der Bevölkerung als problematisch angesehen werden, ist aber entscheidend dafür, dass intelligente Städte reibungslos und effizient funktionieren.

Ein erfolgreicher Angriff auf die Daten der Einwohner einer Stadt führt zu einem Vertrauensverlust in die angebotenen Dienstleistungen und die Administration, was sich beispielsweise auf das Wachstum der Wirtschaft auswirken kann. Von Hackern gestohlene Daten werden oft an Drittparteien weitergegeben, verkauft oder veröffentlicht. Durch diesen Missbrauch persönlicher Daten sind die Einwohner zusätzlichen Cyber-Risiken wie Phishing, Spam, Kreditkartenbetrug oder Identitätsdiebstahl ausgesetzt.

Verfügbarkeit von Daten

Die zunehmende Verbreitung von 4G- und 5G-Netzwerkwerken macht es möglich, grosse Datenmengen schnell zu übertragen. Zudem bieten Technologien wie Long-Range Wireless (LoRa) oder Bluetooth Low Energy (BLE) zusätzliche Datenübertragungsmöglichkeiten, die teilweise nur unzureichend geschützt sind.

Mit dem zunehmenden Datenfluss und der Digitalisierung werden sowohl Organisationen wie auch Einwohner immer abhängiger von der Kommunikationsinfrastruktur: Real-Time-Kommunikation, Zugriff auf webbasierte Applikationen, Sensordaten und Kommunikationsinfrastruktur. Beispiele sind Sensordaten aus dem Strassenverkehr, Stromverbrauch, der Wasserversorgung, Daten aus Luftverkehr und öffentlichem Verkehr oder auch Personendaten der Einwohner.

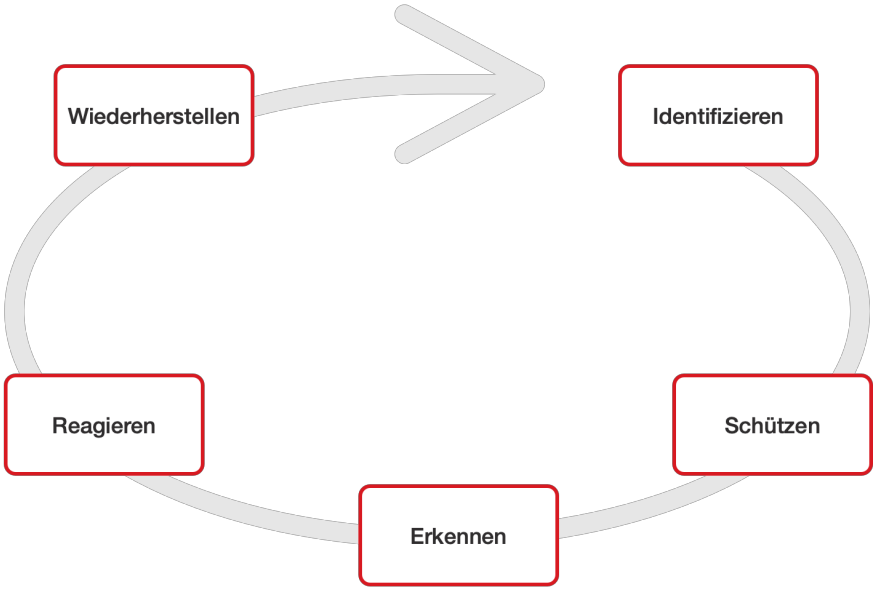
Viele Cyber-Angriffe setzen sogenannte Ransomware ein, um den Zugang auf Daten durch die Verschlüsselung dieser zu verunmöglichen. Kann eine Stadt nicht mehr auf die Daten und Steuerung von Strom- oder Wasserversorgung zugreifen, kann das eine ganze Stadt lahmlegen, der Flugverkehr kann zum Erliegen kommen oder Spitalpatienten können nicht zeitnah versorgt werden. Angreifer nutzen die Situation oft, um Lösegeld zu erpressen, bevor sie die Systeme und Daten wieder freigeben.

Datenintegrität

Smart Cities sind nicht nur darauf angewiesen, dass ihre Daten zugänglich sind, sondern auch, dass diese korrekt sind. Durch die Manipulationen von Daten können Angreifer operative Massnahmen und Kontrollen beeinflussen. Werden Daten zur Wasserqualität in einer Kläranlage manipuliert, kann das zu Gesundheitsrisiken für die Bevölkerung führen. In der Mobilität können falsche Verkehrsdaten einen Stau auslösen, das Pendlerverhalten beeinflussen und Verspätungen verursachen. Sogar nationale Sicherheitsbedrohungen können ausgelöst werden, wenn beispielsweise Sensordaten von Windgeschwindigkeits- oder Strahlungsdetektoren verändert werden und fälschlicherweise ein Alarm und eine Evakuation auslösen oder die Reaktion auf echte Naturkatastrophen verzögern. Manipulierte Daten können der Bevölkerung direkt schaden sowie die Reaktionszeit von Sicherheits- und Rettungsdiensten verlangsamen.

Prävention der Cyberkriminalität

Der Schutz der IT-Systeme ist wichtig, um Vorschriften einzuhalten und zeigen der Bevölkerung, dass ihre verarbeiteten Daten sicher sind. Wenn die Einwohner der Datenverarbeitung vertrauen, kann die Digitalisierung der Stadt aktiv und mit Unterstützung durch die Bevölkerung vorangetrieben werden.



Identifizieren

Der erste Schritt für bessere Informationssicherheit einer Smart City ist die Analyse Ihres IT-Ökosystems: Welche Organisationen, einschliesslich externen Lieferanten, Partner und Dienstleister, sind Teil des Systems? Für die Digitalisierung von städtischen Dienstleistungen werden oft externe Produkte und Services integriert – schliessen Sie gerade diese bei der Analyse ein. Wenn Sie ein Verständnis Ihres IT-Ökosystems haben, identifizieren Sie die Elemente, die für die Stadt und die Bewohner absolut überlebenswichtig sind.

Schützen

Reduzieren Sie potenzielle Angriffsflächen und zeigen Sie Angreifern, dass ein belastbares System vorhanden ist. Achten Sie auch bei angebundenen IT-Produkten und -Services darauf, dass beispielsweise eine End-to-End-Verschlüsselung, Audit-Protokolle, robuste Authentifizierungsmechanismen, aktuelle Antiviren- und Firewall-Software implementiert sind sowie die Möglichkeit besteht, Systeme im Notfall manuell zu überschreiben. Arbeiten Sie mit Experten zusammen, um die Stärke eines Systems zu testen, Sicherheitsrisiken zu identifizieren und Best Practices für die Informationssicherheit zu entwickeln.

Erkennen

Bereiten Sie sich auf Angriffe vor und stellen Sie sicher, dass Fremdzugriffe frühzeitig erkannt und die Verantwortlichen alarmiert werden. Überwachen Sie die Infrastruktur auf verdächtige Aktivitäten und unbefugte Zugriffe. Durch die Antizipation zukünftiger Angriffe ist es Ihrer Smart City möglich, die Einsatzbereitschaft aller Bereiche jederzeit sicherzustellen.

Reagieren

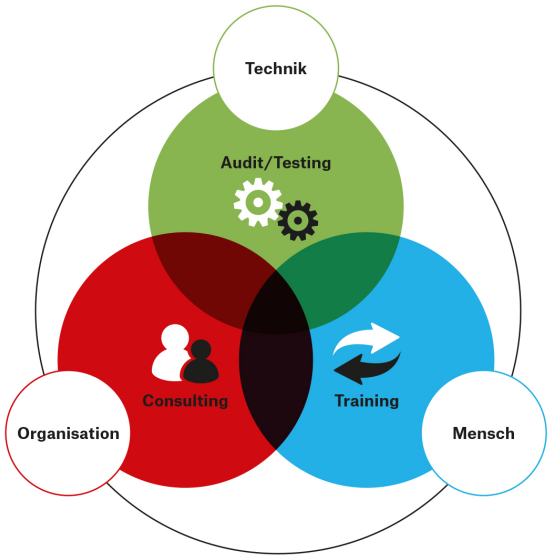
Angriffe können Sie zwar nicht kontrollieren – die Reaktion darauf aber schon. Bauen Sie Failover-Server und -Systeme auf, auf die Sie ausweichen können, wenn wichtige Server und Dienste Ihrer Stadt durch Hacker beeinträchtigt oder gar übernommen wurden. Failover-Szenarien sollten in einem gut ausgebildeten und ausgestatteten Security Operations Center (SOC) verwaltet werden – entweder Inhouse oder durch einen externen Dienstleister. Das SOC priorisiert im Krisenfalls die Gegenmassnahmen, unterstützt die Regierung beim effektiven Risikomanagement und hilft, fundierte Entscheidungen im Sicherheitsbereich zu treffen.

Wiederherstellen

Die Cyber-Angriffe entwickelt sich stetig weiter – deshalb ist ein kontinuierlicher Verbesserungszyklus wichtig. Analysieren Sie Cyber-Angriffe und nutzen Sie Erfahrungen für die stetige Weiterentwicklung und regelmässige Analyse Ihrer IT-Security.

Informationssicherheit im Gesamtkontext

Zur Informationssicherheit – die Vertraulichkeit, Integrität und Verfügbarkeit von Informationen – gehören die technischen Systeme, die Prozesse einer Organisation sowie die involvierten Menschen. Jeder dieser Aspekte birgt potenzielle Risiken und Schwachstellen. Durch die starke gegenseitige Abhängigkeit ist es wichtig, dass Sie Informationssicherheit nicht nur punktuell adressieren, sondern ein übergreifendes Information Security Management System aufbauen, das alle Aspekte miteinander vereint.



Prozesse: Klare Verantwortlichkeiten und Abläufe

Informationssicherheit hängt stark von den bestehenden Prozessen und Funktionen einer Organisation ab, sowie die der angebundenen Dienstleister. Öffentliche Bauzonenpläne, Mobilitätstatistiken und Informationen zu Naturschutzobjekten – sogenannte «Open Data» – sind ein passendes Beispiel dafür. Wer betreibt diese Plattformen und wer ist für falsche – durch einen Angriff publizierte – Daten verantwortlich oder gar haftbar? Die Stadt oder ein externer Lieferant? Klären Sie Zuständigkeiten, sodass die Verantwortlichen sicherstellen können, dass die Integrität, Verfügbarkeit und Vertraulichkeit von Daten gewährleistet sind. Die Feuerwehr weiss bei einem Brand genau, wer was zu tun hat – genau gleich müssen Sie auch für Cyber-Sicherheitsvorfälle Prozesse definieren, die im Notfall aktiviert werden und eingeübt sind.

Situationsanalyse evaluiert Ihre Prozesse

Lassen Sie Ihr ICT-Ökosystem und Ihre Sicherheitsprozesse von Security-Experten analysieren. Redguard identifiziert potenzielle Risiken und Schwachstellen und hilft Ihnen, diese zu beheben. Gerne unterstützen wir auch bei der Umsetzung des vom Bund und Branchenverbänden empfohlenen IKT-Minimalstandards.

Technik: Technologische Möglichkeiten sicher umsetzen

Die Technologie bietet stetig neue Möglichkeiten für Smart Cities – und für Angreifer. Beispielsweise sind drahtlose Kommunikationsschnittstellen ein attraktiver Angriffspunkt, wenn diese nicht entsprechend verschlüsselt sind. Zudem sollten Systeme regelmässige Security Updates erhalten, auch dezentrale Hardware wie Sensoren. Regelmässige Sicherheitstests durch Spezialisten können zudem Schwachstellen in der Programmierung von Systemen und Konfiguration von Netzwerken aufdecken und auch sogenannte «Blindspots» identifizieren. Durch konkrete Handlungsempfehlungen aus Tests und Simulationen können Schwachstellen frühzeitig und effizient behoben werden.

Attack Simulation

Ihre Technik, Prozesse und Mitarbeitenden werden auf die Probe gestellt: Wir simulieren einen realen Cyber-Angriff und versuchen in enger Zusammenarbeit mit Ihnen, Ihre Daten zu stehlen, Systeme lahmzulegen oder in Räumlichkeiten einzudringen. Mit unseren Risikobeurteilungen und Empfehlungen steigern Sie Ihre Informationssicherheit.

Mensch: Bewusstsein stärken

Die Sicherheit eines Systems ist stark von dessen Anwender und Betreiber abhängig. Die beste Firewall nützt wenig, wenn schwache Passwörter gesetzt sind oder wenn vertrauliche Daten fahrlässig behandelt werden. Häufig ist es Mitarbeitenden nicht bewusst, welche Auswirkungen scheinbar triviale Verhaltensweisen haben können oder welche rechtlichen Vorschriften bezüglich des Datenschutzes gelten. Wird das Bewusstsein der Mitarbeitenden für Informationssicherheit geschult, kann oftmals mit kleinem Aufwand eine grosse Verbesserung erreicht werden und die Mitarbeitenden erhalten mehr Sicherheit im täglichen Umgang mit Sicherheitsthemen.

Security Awareness Training

Menschliche Verhaltensweise im Bezug auf Informationssicherheit stehen im Zentrum. Wir schulen Ihre Mitarbeitenden im Bereich Informationssicherheit: Den sicheren Umgang mit Daten und Systemen, die Umsetzung von Prozessen sowie aktuelle Sicherheitsrisiken. Das stärkt das Bewusstsein und so die Sicherheit Ihrer Organisation.

Verbessern Sie die Cyber-Sicherheit in Ihrer Smart City

Als schweizweit führender Dienstleister im Bereich der Informationssicherheit unterstützt Sie Redguard dabei, Ihre Informationssicherheit zu verbessern. Durch die langjährige Zusammenarbeit mit dem Bund, Kommunen sowie Technologieunternehmen kennen wir die Anforderungen von Smart Cities und die aktuellen Sicherheitsherausforderungen. Als unabhängiges und neutrales Unternehmen mit qualifizierten Security Testern und Consultants analysieren wir Ihre Systeme und Prozesse und liefern konkrete Handlungsempfehlungen zur Erhöhung der Sicherheit in Ihrer Smart City.

Kontakt

Ihre Werte zu schützen – dieses Ziel steht im Fokus
Wir unterstützen Sie gerne mit Audits/Testing, Consulting und Trainings.

Dominique Meier, Head of Operations bei Redguard
contact@redguard.ch
+41 31 511 37 50