through systems that are not properly segmented. IT experts are needed – and they need to continually update their skills.

Operational co-operation and cross-divisional collaboration are also important. Especially in the public sector, resources need to be used efficiently and effectively. With regard to cybersecurity, this can help achieve a higher level of protection overall. For complex IT systems, such as those in smart communities, to work securely together, the different units need to be connected. Information needs to flow – and to actually be used as well as processed. Vertical and horizontal networking is needed.

Dynamically changing environments require continuous improvement. Learning from internal and external mistakes is essential to keep up with these developments. Innovations as well as paradigm shifts are the norm, especially in the digital world. It is necessary to make learning an integral part of the organisational culture. In the field of IT this is nothing new and is usually referred to in the form of maturity models. However, we believe that this needs to be rooted at the heart of the entire organisation and smart community.

We will continue our research in this field in the coming months as part of the current project and hope to expand on it in the future.

References

[1] G. R. Wollinger and A. Schulze Eds.: "Handbuch Cybersecurity für die öffentliche Verwaltung, Wiesbaden: Kommunal- und Schul-Verlag, 2020", [online] available: https://kwz.me/h8a

[2] J. Remy and R. Stettner: "Cybersicherheit als Aufgabe der Länder," Datenschutz Datensich, vol. 45, no. 4, pp. 254–258, 2021, doi: 10.1007/s11623-021-1429-y.

Please contact:
Kirstin Scheel
Fraunhofer Institute for Secure Information Technology SIT, Germany
kirstin.scheel@sit.fraunhofer.de
+49 6151 869 268

Policies and Recommendations for IT Security in Urban Environments from the Morgenstadt Urban Data Partnership Project

by Philipp Lämmel, Michell Boerger, Nikolay Tcholtchev (Fraunhofer FOKUS) and Eva Ottendörfer (Fraunhofer IAO)

Urban ICT infrastructure is playing an increasingly decisive role as the technical backbone of smart cities. To guarantee the protection of the public sector and citizens in this context, the security of this infrastructure is of utmost importance and should be continuously monitored and improved. This article presents measures and recommendations towards ensuring the security of urban ICT infrastructures.

The smart cities domain is becoming ever more relevant for our society. The accelerating digitalisation of processes in urban settings is expected to lead to long-term improvements, enhancing the quality of life of inhabitants and creating more liveable, sustainable, and inclusive cities. Information and communications technology (ICT) plays an essential role as the backbone of digital transformation. New optimisation opportunities are arising due to the ICT-enabled emerging capabilities for combining and evaluating new services and data sources. In addition, digitalisation and the accompanying transformation of the economy and our everyday lives offer the potential to optimise fundamental urban processes, e.g. in the domains of mobility, transportation and energy.

To ensure that cities and communities do not have to face these diverse challenges on their own, the Urban Data Partnership (UDP) was founded by the Fraunhofer Morgenstadt network [L1]. One aim of this initiative is to stimulate the transfer of knowledge between cities/communities by creating common knowledge as well as sharing experience and strategies regarding the efficient and secure management of urban data. In the long term, the UDP aims to accelerate the digital transformation of cities and communities, while considering (data) security in an urban environment. Based on knowledge gleaned from the UDP, this article presents measures and recommendations to ensure the security of urban ICT services and systems in smart urban environments. The fundamental policies and recommendations are discussed below and summarised in Figure 1.

Stakeholder engagement and governance

An open ecosystem of diverse stakeholders who are aware of the importance of cybersecurity in a smart city is a fundamental driver for the sustainable and secure implementation of smart urban use cases. Therefore, all stakeholders, including the city government, should be encouraged from the beginning to create a culture of cybersecurity throughout all the involved public entities.

Apply security frameworks and standards

To secure a smart city/community, the security of the ICT infrastructure must be addressed as early as the conception phase. Security is important at every step of the development lifecycle and vulnerabilities should be avoided at every level. To this end, the National Institute of Standards and Technology (NIST) has published a cybersecurity framework [1] covering many topics. This framework is a must-read for anyone involved or interested in improving security in their city, community or organisation.

In addition, in 2002, the OECD published revised guidelines for informa-

tion systems and network security, underpinned by nine principles [2]: (1) awareness, (2) responsibility, (3) response, (4) ethics, (5) democracy, (6) risk assessment, (7) security design and implementation, (8) security management, and (9) reassessment. NIST expanded upon these principles in their document Systems Security Engineering: Considerations for a Multidisciplinary Approach in the Engineering of Trustworthy Secure Systems [3]. This document provides a taxonomy of security design principles to be used as a basis for engineering trustworthy, reliable, and secure systems.

Avoid known security vulnerabilities and threats

Since software is becoming increasingly complex and interconnected, the difficulty of achieving application security is also increasing exponentially. Therefore, the Open Web Application Security Project (OWASP) published the ten most critical security risks for web applications [L2]. These have become the de facto standard for application security. We recommend that all actors involved in developing an urban ICT infrastructure study the risks and resulting measures identified by the OWASP.

Cover security basics

The following security basics should be followed:

- On-time software updates: All software used in an urban ICT environment should be kept up to date, so that no known security vulnerabilities can be exploited. All firewalls and antivirus programs should be updated regularly.
- Enforce secure passwords and policies: Users should regularly update their passwords to ensure that they are unique and complex. Strict policies should be enforced to ensure that passwords are secure. Furthermore, establishing security operation centres could be helpful to monitor security, mitigate vulnerabilities, and respond to attacks.
- Correct operating procedures: Deploying firewalls is an important step in protecting a smart city/community. Determining the type of traffic allowed to pass through the firewall is one of the most central ways to protect a network from potential attacks.

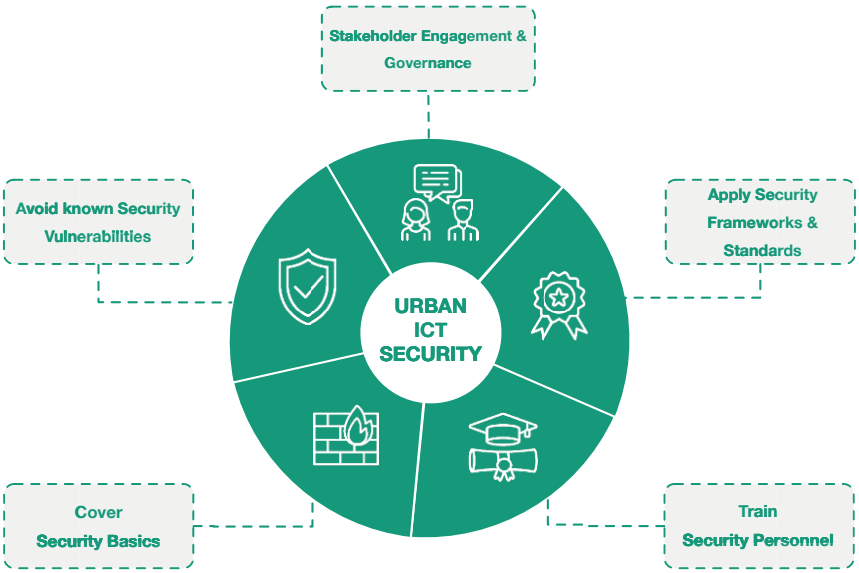

Figure 1: Overview of identified measures and recommendations which are crucial for ensuring the security of urban ICT services and systems.

- Strong access controls: All systems that are not currently in use should be disabled. Unused remote management functions and ports should also be disabled to prevent attackers from accessing them. Furthermore, network activities should be scanned regularly, and suspicious internet traffic should be monitored with the help of security incident and event management tools to detect attacks at an early stage.

Train security personnel

A further security-related challenge is the training of staff to secure an urban infrastructure. Due to the rapid growth and expansion of smart cities, there is currently a shortage of security experts in the urban context. Therefore, the training and certification of professionals for the development, construction, operation, and maintenance of urban ICT infrastructures should be urgently promoted.

Summary

In summary, particular policies and recommendations should be followed for the secure implementation and operation of urban ICT infrastructures, namely: stakeholder engagement and governance; application of security frameworks and standards; avoidance of known security vulnerabilities; training of personnel; coverage of security basics; and the establishment of adequate security processes.

Links:

[L1] https://kwz.me/h79
[L2] https://kwz.me/h7f

References:

[1] NIST, "Framework for Improving Critical Infrastructure Cybersecurity, Version 1.1," National Institute of Standards and Technology, Gaithersburg, MD, NIST CSWP 04162018, Apr. 2018. DOI: 10.6028/NIST.CSWP.04162018.
[2] OECD Guidelines for the Security of Information Systems and Networks. OECD Publishing, 2002. doi: 10.1787/9789264059177-en-fr.
[3] R. Ross et al., "Systems Security Engineering: Considerations for a Multidisciplinary Approach in the Engineering of Trustworthy Secure Systems," National Institute of Standards and Technology, NIST SP 800-160, Nov. 2016. DOI: 10.6028/NIST.SP.800-160.

Please contact:

Philipp Lämmel
Fraunhofer Institute for Open Communication Systems FOKUS, Germany
philipp.laemmel@fokus.fraunhofer.de