Communication Papers of the of the 17th Conference on Computer Science and Intelligence Systems pp. 183–189
DOI: 10.15439/2022F162
ISSN 2300-5963 ACSIS, Vol. 32

Information security management in German local government

Frank Moses, Kurt Sandkuhl
University of Rostock, Institute of Computer Science, Albert-Einstein-Str. 22, 18057 Rostock, Germany Email: {frank.moses, kurt.sandkuhl}@uni-rostock.de

Thomas Kemmerich
University of Bremen, TZI
Bibliothekstraße 1, 28359 Bremen, Germany Email: Thomas.kemmerich@uni-bremen.de

Abstract—**The growing importance of information security in organizations is undisputed. This is particularly true of local governments, because modern administrative action is no longer conceivable today without electronic communication media and IT procedures. The complexity of information technology, the increasing degree of networking (also with citizens) and the dependence of the administration on IT-supported procedures has led to the fact that the security of information technology and associated processes must be given a higher priority and a corresponding cybersecurity strategy must be substantiated. Existing approaches either fall short or cannot be applied to the context of local government without revision and adaptation. In this article, case studies of implementations of IT security projects in local government are examined. Specific focus is on the differences between information security management system (ISMS) implementations of different hierarchical levels of governmental organizations. The results show current challenges in increasing the resilience of the local government.**

I. Introduction

INFORMATION security is a comparatively new topic in the domain of local government. The automated processing of data and information now plays a key role in the fulfilment of tasks in small and medium-sized enterprises (SMEs) and also in local governments [1, S. 429–431, 435], [2, S. 1]. All essential processes are significantly supported by information and communication technology (ICT) [3, S. 137f.]. Furthermore, legal requirements such as the General Data Protection Regulation (EU-GDPR), the Online Access Act (OZG) and the E-Government Act are driving forces of digitization in the domain. [4], [5], [6].

Increased reliance on modern ICT has significantly increased the risk of information infrastructures being adversely affected by deliberate attacks from inside and outside, negligent action, ignorance or technical failure, both qualitatively and quantitatively.[7, S. 86 u. 107], [8, S. 196]. Lack of information security can lead to disruptions in the performance of tasks, which can reduce the performance of authorities and, in extreme cases, bring their business processes to a standstill [9, S. 688]. Against this background, ensuring information security is one of the central tasks of local governments, within the framework of which an appropriate level of security in business processes and the associated (IT) infrastructures must be organized. [10, S. 650]. This need is underlined in particular by the recent successful cyber-attacks in various federal states, especially against authorities [11], [12]. Public authorities in particular are institutions of high importance for the state community. Impairments or failures may result in public service shortages, significant disruption of public security or other serious consequences [13]. In order to study the information security of local governments, a case study analysis was carried out. The aim of the work descripted here is to identify the state of information security of local governments and critical public infrastructures in order to contribute to the research field of information security in the domain of local government. Specific focus is on the differences between information security management system (ISMS) implementations of different hierarchical levels of governmental organizations.

II. Research Method

Work presented in this paper is part of a PhD project aiming at methodological and technological support for information security management that is tailored to the needs of small and medium-sized local government units. The PhD project follows the paradigm of design science research [14] and started with an analysis of (a) existing scientific work in the field of information security management (ISM) for local governments and (b) an analysis of typical problems in local government's ISM as visible in information security audit reports. The detailed results of both steps are available in [15]; the literature analysis is summarized in section III.

As the audit reports analyzed in (b) mainly reflected shortcomings of ISM implementations, we decided to also look for successful elements of ISM implementations by analyzing ISM cases. This paper focuses on these cases that – in a DSR context - contribute to the investigation of problem relevance and to requirements for the envisioned artifact. The research question for this work is: What are the differences (if any) between ISMS implementations of different kind and hierarchical levels of governmental organizations?

The introduction of information security management systems (ISM) usually represents an intervention in existing business processes and is influenced by various success factors. Case studies and retrospective analyses are research strategies [16] for qualitative data collection, which are very well suited to investigate the complex issues in the real environment [17]. Methods of qualitative data analysis help to understand process sequences and the dynamics of concrete situations under certain framework conditions and to derive results from them [18].

Thus, we analyzed various ISM cases. Although our cases show many characteristics of qualitative case studies as described by [16] (e.g., defined boundaries, defined research question, rich set of qualitative material, etc.), we prefer the term "ISM case", because most of the case material was not collected with the case study research method in mind but evaluated ex-post as case material. Here, eXperience methodology [19] supports the research work on the one hand in the uniform preparation of the ISM cases and on the other hand it can be ensured that the ISM cases are made comparable in order to derive concrete results from them.

III. Summary of Literature Analysis

In order to identify relevant literature on the status-of-research of ISM in local government sector, a structured literature search was carried out following [6]. The literature search was conducted in the databases EBSCO EconLit and WISO (Public Ser-vice, Business Administration), SSOAR (Administrative Sciences) and Scopus (various scientific disciplines) with a combination of the search terms: "cybersecurity, public sector, information security". In addition, references to relevant systematic works from the publication period 2013 to 2021 were reviewed.

The initial search resulted in more than 1,500 hits, which were in several steps reduced to 85 articles by examining the titles, keywords and abstract. It followed an assessment of their relevance using the content, quality and citation frequency. Finally, 26 papers were classified relevant and grouped into thematic areas. Table I shows these areas and the relevant papers.

Table I.
Relevant literature sorted into thematic areas

Thematic area	Literature
Validation of technical components	[20], [21]
Analysis of factors hindering the development of cybersecurity strategies in the public sector	[22]
Analysis of cyber attacks and preventive measures	[23], [24], [25], [26]
Development an establishment of ISMS	[27]
Awareness measures	[28], [29], [30], [31], [32], [33]
Lack of skilled workers in public sector and effects	[34], [35]
Physical Security and Security Assessment	[36], [37], [38], [39], [40]
Legal framework parameters in cybersecurity domain	[41], [42]
Maturity models	[43], [44]

Most papers deal with the safeguarding of the technical components or tackle the analysis of cyber-attacks and possible preventive measures. It is striking that a large number of papers put the staff in the focus and examine how their awareness for cybersecurity can be increased.

Also, a substantial number of papers address options for the protection of physical security and security assessments and discuss the lack of skilled workers in the public sector.

Furthermore, papers regarding the legal frame-work and digital sovereignty must be mentioned.

Since the introduction of EU-GDPR in 2018, information and cybersecurity have been used more and more synonymously and very often set in relation to data protection and data protection issues. In contrast, only one relevant article addresses the structure and establishment of ISM systems.

IV. ISM Cases

Although the topic of information security in local government has only recently been given more attention in Germany, corresponding concepts for the development and establishment of information security management systems already exist [45], [46]. With support of these concepts, a few local governments have already dealt with the topic of information security and set up a corresponding management system.

The municipalities examined in the focus of this research are mainly in the two federal states of Germany, namely Bavaria and Saarland. These organizations are motivated by funding programs of the respective state government to introduce and operate a corresponding security management system.

A. Case material

One of the authors supervises various institutions in setting up Information Security Management systems to increase the resiliency of the respective organization. The associated ISM cases were conducted in the years 2018 to 2022 and cover a wide range of state, city and local government and an SME as well as a critical infrastructure from four federal states.

Various municipal organizations throughout Germany were asked to participate in the ISM cases. In addition, further municipal case study participants from other federal states without a funding program and three medium-sized companies were sought as a comparison group who were willing to have the development of their information security management system scientifically accompanied. The cases consist of local governments (small to medium-sized), district council offices, city administrations, state companies, state administration and a company as well as a hospital network. For this contribution, 24 ISM cases were selected that exemplify the situation in German local government.

In all ISM cases, the documentation of ISMS, including organization structure and processes were available and analyzed. Furthermore, access to the stakeholders in the organization was possible to collect required information from other reports. This was used during ISM case analysis.

TABLE II.
ISM CASES ANALYZED IN THIS PAPER

No.	Governmental Organization	Federal State	Type of organization
1	Gemeinde ****dorf	BY	Local government
2	Gemeinde Ma******	SL	Local government
3	Gemeinde Post*****-****	BY	Local government
4	Landeshauptkasse Saarland	SL	State administration
5	Zentrales Travelmanagement Saarland	SL	State administration
6	Landratsamt Frei****	BY	District Office
7	Landratsamt Neu*****	BY	District Office
8	LEG-Service GmbH	SL	Enterprise
9	Markt ***bach	BY	Local government
10	Markt ******dorf	BY	Local government
11	Performa Nord GmbH	HB	Enterprise
12	SlyCon GmbH	SL	SME
13	Stadt Hi****	NW	Municipality
14	Stadt ***heim	BY	Municipality
15	Stadt Neuburg a.d. Donau	BY	Municipality
16	Stadt *******furt	BY	Municipality
17	Stadt S*****fen	BY	Municipality
18	Stadt St. *******	SL	Municipality
19	Stadt ****bach	SL	Municipality
20	Stadt *******hausen	BY	Municipality
21	Stadtwerke *******hausen	BY	Municipal Utilities (critical)
22	Stadt *****burg	BY	Municipality
23	VG Neumarkt i.d. Oberpfalz	BY	Local government
24	VG ****beuren	BY	Local government

B. Coding for Cross-Case Analysis

The cases listed in the previous section cover different hierarchical levels of local government and also different IT security areas. The aim of the case analysis was to identify patterns, similarities and differences in the cases, which allow conclusions to be drawn about generally valid relationships, proven process models and framework conditions relevant for success.

The case material was examined. In order to give the analysis more significance, the following criteria were coded in advance according to Mayring [48], followed by a content analysis of the case material so that corresponding core statements could be derived. The following describes the coding.

TABLE III.
CODING SCHEME FOR THE QUALITATIVE CONTENT ANALYSIS OF THE ISM CASES

No.	Coding
1	Managementattention
2	Leadership
3	Organizational structure
4	Process organization
5	Employee awareness
6	PDCA-Cycle
7	Guidelines and other documentation tasks
8	Use of tools (ISMS-Tools, Controlling-Tools, usw.)
9	Implementation of measures (Increased IT security)
10	Risk management
11	CIP process (Assessment and measurement)

Management attention (Coding 1): Essential for the development of an information security management system is the assumption of the responsibility of the management level for the topic per se [45, S. 7], [49, S. 24–27]. Against this background, the analysis focused on the extent to which the respective management level was involved in the ISMS process.

Leadership (Coding 2): The management initiative is the basic prerequisite for successfully setting up an ISMS in an organization. Nevertheless, the complex topic of ISMS requires concrete control and management tasks, which in the best case are taken over by the management itself or delegated accordingly and then performed.

Organizational structure (Coding 3): The planning and implementation of the security process includes the definition of organizational structures and the definition of roles and tasks [45, S. 28]. With this coding, all places in the ISM cases are marked, which provide information regarding the organizational structure in the context of security concept.

Process organization (Coding 4): Many tasks in organizations are organized as processes, with a specific process owner, a person in charge, and a description. The structure of a security management system includes in particular the recurring processing of maintenance, fault and change processes. The qualitative implementation of these processes form the foundation of an ISMS and are therefore marked with code 4.

Employee awareness (Coding 5): Especially the recent attacks on public infrastructures have shown that a gateway is formed by the employees of the organization itself. [7, S. 54] and these must be sensitized accordingly [50]. Against this background, it is interesting to find out which measures have been planned and implemented by the organizations with regard to employee awareness.

PDCA-Cycle (Cycle 6): A management system thrives on the recurring sequence of planning, implementation, review and initiation of corrective measures [45, S. 17]. In the analysis of the ISM cases, great emphasis was placed on coding No. 6. Essentially, it is a matter of determining whether only an ISMS is being set up in order to obtain a one-time certificate or whether the organization operates the ISMS sustainably.

Guidelines and Documentation task (Coding 7): The documentation task is indispensable [45, S. 21] and in an ISMS project ranges from the guideline for information security, through further planning and guideline documents to clear process descriptions and verification documents. It is precisely this documentation task that poses major challenges for small and medium-sized enterprises as well as for local governments. Policy documents belong to the PDCA cycle planning category, and without a good plan, the goal is often not achieved. Therefore, as part of the analysis of the ISM cases, exactly this component of an ISMS will be analyzed.

Use of tools (Coding 8): Within the framework of an ISMS project, there is a need for tool support for the ISMS as well as for other tasks within the framework of the security concept, e.g. monitoring of network activities with the help of special tools. Especially the use of tools is an important success factor in order to fulfill or monitor the multitude of different tasks. Against this background, statements regarding the use of tools are coded accordingly.

Implementation of measures (Coding 9): A holistic ISMS pursues the goal of implementing and planning both preventive measures and measures to remedy security incidents. When analyzing the ISM cases, it is to be examined which type of measures (organizational, personnel, infrastructural and technical security measures) have been planned and implemented and what contribution they make to increasing security.

Risk management (Coding 10): The operation of any process or IT infrastructure is associated with risks. The risk management process is thus one of the foundations of a security management system [51, S. 7]. Experience has shown that risk identification and treatment is particularly difficult for local governments. To identify how risk management is embedded in the security process, Coding 10 will play an important role in the analysis of the ISM cases.

Continuous improvement - CIP (Coding 11): In order to maintain information security, it must be subject to permanent improvement. Logically, this necessitates continuous measurement and, above all, evaluation. [46]. How and with which results the CIP process was implemented in the respective ISM cases is marked with the code 11 and later evaluated accordingly.

V. Case Analysis

A. *Groups of Cases and their Difference*

Based on the coding and analysis of the available case material, groups of governmental organizations were identified and differences in their ISM implementations recognized. These groups are summarized in the following.

Local Government cases – Adoption and Diffusion of an ISMS

The eight ISM cases from the domain of local government essentially address the challenges of setting up and establishing an information security management system in a small administrative organization (max. 25 employees). At the same time, these "small" local governments have to meet the increased demands on administrative processes due to increasing digitization. Furthermore, due to the tight tariff structure of the public service, organizations are often unable to engage employees with the appropriate qualifications, so that in addition to IT technology, both internal and cross-organizational challenges have been identified that must be solved for successful implementation. Furthermore, the documentation task is one of the biggest challenges in small local governments. In addition, there is a lack of suitable tools that support the development and establishment of the information security management system for this target group.

District Administration cases – Implementation of the Security Requirement

In the case of the two ISM cases from the domain of district administration, a different picture emerges. The necessary human and financial resources are available here. Nevertheless, additional tasks have to be performed within this domain, which are necessary as a service for the subordinate administrative levels. The ISM cases focused on the challenges that arise from the development of an information security management system in organizations. Essentially, in large administrative organizations, the management attention and the role definition and process descriptions, especially in the IT and security domain, are suboptimal. Due to hierarchical levels with in parts of a wide lead span, losses occur at the organizational interfaces (structure and process organization). Furthermore, the involvement of stakeholders and their training and sensitization as well as employees for the requirements of information security is a major challenge.

City Administration cases – Security in Organizational Processes

The eight city administrations have to cope with different challenges in terms of IT security compared to other municipal organizations. The processing of sensitive (often private) data requires a particularly secure handling of this data. Based on the introduced information security management system, the established strategy is supplemented by modern measures for data backup and process automation. Furthermore, the maturity level derived from the information security management system can be used to obtain data that can be used to support further management decisions. For example, it can be used to secure make-it or buy-it decisions that have the goal of outsourcing certain services, both for economic and security reasons. Furthermore, this strategy replaces heterogeneous risk landscape in favor of new uniform risk assessments. The use of suitable tools to support the ISMS process was essential in these ISM cases.

State Administration cases – Secure Business Processes for Financial and Travel Transactions

The ISM cases use the example of a "state accounting" and central travel management to describe the challenges there in the context of IT security. In addition to the administration of a large amount of private data within the scope of the tasks of the travel management process, the business process " state accounting " in particular forms a core process of a state administration. In this process, all bookings of a state administration converge. Many interfaces (e.g. with banks, debtors and creditors) have to be secured both organizationally, contractually and technically. The information security management system, which has been established in the meantime, forms the foundation for further strategies to secure information security, especially in the area of payment transactions and travel management. This is based on advanced risk management, which provides a dashboard that aggregates and provides data from different sources. The C-Level-Management is now in a position to identify and treat aggregated risks that were previously not the focus of the implementation of measures as individual risks.

National Company case – IT Security at an Airport Operator

The main focus of the ISM case at an airport operator are the reactions of the ransomware attack that took place there in autumn 2020. This attack has given the impetus to implement planned measures more quickly.

At the same time, the attack and the associated ransom demand have increased the management attention accordingly. As a result, both human and financial resources were made available to build up the non-existent risk management and to promote the implementation of measures to increase IT security.

The forensic analysis revealed that a lack of employee sensitization and training and, partly, organizational failure were one of the main causes of the successful cyberattack. As a result, the following points can be mentioned in order to better defend against targeted attacks on a critical infrastructure in the future:

- Implementation of a sustainable organization-wide IT security concept,
- Streamline the threat detection process and
- Increase in the ability to deal with threats,
- Further establishment of an open cooperation of all those responsible and
- Use of suitable tools (e.g. monitoring PDCA cycle, risk and maturity model)

Clinic Network case – IT Security at a Hospital Network and Municipal Utilities

Another ISM case was carried out in a clinic network. German hospitals, as part of the public critical infrastructure, are motivated on the one hand by various successful cyberattacks against hospital infrastructures on the other hand by legal requirements to introduce an information security management system [47, S. 196]. The central topic of the ISM case in the hospital network and in the critical infrastructure of the municipal utilities examined is the use of suitable tools that accompany and optimize the introduction and implementation of a information security management system taking into account different standards (e.g. BSI Compendium 2022 and the B3S[1] of the German Hospital Association).

B. Application of Coding Scheme

Using the coding presented in section IV.b. all ISM cases were examined with respect to the maturity the individual case showed for the aspect represented by the coding. The maturity levels used were from level 1 (low maturity – only basic implementation) to level 5 (high maturity - managed and optimized status). All ISM cases focused on the introduction of an information security management system to increase the resiliency against cyber-attacks of the respective organization.

As part of the ISM cases, a prototypical process model developed by one of the authors was used [52, S. 61ff]. This process model attempts to eliminate the shortcomings that have been revealed in the analysis of the audit reports. In essence, a positive result was achieved for all facilities. Some of the above-mentioned organizations have already successfully passed an audit; others are still working towards it.

An analysis of the audit reports of the subjects from the ISM cases as well as the ISM cases themselves showed a significant improvement in the individual codes. Thus, a strong improvement in the maturity level of the information security management system and organizational resilience can be observed. The results can be found in Table IV.

TABLE IV.
DISTRIBUTION OF MATURITY LEVELS IN THE ISM CASES FOR THE DIFFERENT CODING[2]

	Distribution of encodings in %				
Coding	1	2	3	4	5
1	4,2	8,3	58,3	20,8	8,3
2	4,2	8,3	66,7	12,5	8,3
3	0,0	12,5	75,0	8,3	4,2
4	8,3	20,8	50,0	16,7	4,2
5	4,2	8,3	45,8	29,2	12,5
6	4,2	20,8	41,7	29,2	4,2
7	0,0	4,2	37,5	54,2	4,2
8	0,0	0,0	20,8	75,0	4,2
9	0,0	0,0	41,7	50,0	8,3
10	4,2	20,8	54,2	16,7	4,2
11	8,3	8,3	62,5	16,7	4,2

VI. SUMMARY AND DISCUSSION

24 ISM cases were carried out, which qualitatively examined projects to increase IT security, IT security concepts or individual IT security measures of different levels of German local governments from four federal states.

A prototypical procedure was used for the supported organizations, which enables the organizations to implement corresponding projects to ensure information security in a practicable way. At the same time, a basis was created for incorporating the findings made in the preliminary analysis into

[1] B3S – Branch-Specific Security Standard

[2] Values are rounded to one decimal place.

the process model. As a result, the respective organization is supported organizationally, technically as well as structurally.

In order to identify patterns in the ISM case series, a cross-case analysis in the form of a qualitative content analysis according to Mayring was carried out after the completion of the projects.

To secure the process model, this was also applied in a domain outside the local government. The results obtained confirm the findings from the primary research domain.

This article contributes to the understanding of the overall context of successful IT security projects for the implementation of IT security concepts in local government.

For the present work, the methodological limitations of case studies apply. Nevertheless, the generalizability of the results is possible, which the comparison group with 3 companies has shown. Further research will show whether qualitative and quantitative research based on this confirms the similarities and differences found.

One of the biggest limitations of our work is the focus on German local governments when it comes to the ISM cases used. The conclusions drawn from this material cannot be transferred to other countries but might help to identify the focus of attention for future analysis efforts in other federal governmental structures. However, this limitation does not apply for the analysis of the state-of-research, i.e., we see a clear need for more research on ISM in small and medium-sized governmental units.

References

[1] A. Schönbohm, „Flexibilität und Unabhängigkeit - Rahmenbedingungen für eine gesellschaftliche Cyber-Sicherheit“, in Digitalisierung im Spannungs-feld von Politik, Wirtschaft, Wissenschaft und Recht, Bd. 1, C. Bär, T. Gräd-ler, und R. Mayr, Hrsg. Berlin: Springer Gabler, 2018.

[2] S. Mierowski, Datenschutz nach DS-GVO und Informationssicherheit gewährleisten: eine kompakte Praxishilfe zur Maßnahmenauswahl: Prozess ZAWAS 4.0. Wiesbaden: Springer Vieweg, 2021.

[3] H. Gulden, „Digitalisierung und IT-Sicherheit“, in Digitalisierung im Spannungsfeld von Politik, Wirtschaft, Wissenschaft und Recht, Bd. 1, C. Bär, T. Grädler, und R. Mayr, Hrsg. Berlin: Springer Gabler, 2018.

[4] VERORDNUNG (EU) 2016/679 DES EUROPÄISCHEN PARLAMENTS UND DES RATES. 2016. Zugegriffen: 27. Oktober 2021. [Online]. Verfügbar unter: https://eur-lex.europa.eu/legal-content/DE/TXT/HTML/?uri=CELEX:02016R0679-20160504&from=DE

[5] OZG - Gesetz zur Verbesserung des Onlinezugangs zu Verwaltungsleistungen. Zugegriffen: 27. Oktober 2021. [Online]. Verfügbar unter: https://www.gesetze-im-internet.de/ozg/

[6] EGovG - Gesetz zur Förderung der elektronischen Verwaltung. Zugegriffen: 27. Oktober 2021. [Online]. Verfügbar unter: https://www.gesetze-im-internet.de/egovg/BJNR274910013.html

[7] D. C. Leeser, Digitalisierung in KMU kompakt: Compliance und IT-Security. Berlin [Heidelberg]: Springer Vieweg, 2020. doi: 10.1007/978-3-662-59738-5.

[8] N. Pohlmann, „Ohne IT-Sicherheit gelingt keine nachhaltige Digitalisierung“, in Digitalisierung im Spannungsfeld von Politik, Wirtschaft, Wissenschaft und Recht, Bd. 1, C. Bär, T. Grädler, und R. Mayr, Hrsg. Berlin: Springer Gabler, 2018.

[9] I. Henseler-Unger und A. Hillebrand, „Aktuelle Lage der IT-Sicherheit in KMU: Wie kann man die Umsetzungslücke schließen?“, Datenschutz Daten-sicherheit - DuD, Bd. 42, Nr. 11, S. 686–690, Nov. 2018, doi: 10.1007/s11623-018-1025-y.

[10] D. Kammerloher, „Cybersecurity: Ein sicheres Fundament für den digitalen Staat“, Datenschutz Datensicherheit - DuD, Bd. 45, Nr. 10, S. 649–653, Okt. 2021, doi: 10.1007/s11623-021-1508-0.

[11] Gernot Heller, „Immer mehr Cyberangriffe: IT-Sicherheitsbehörde BSI schlägt Alarm - Professionalität steigt: IT-Sicherheitsbehörde BSI schlägt Alarm - Professionalität steigt“, Passau. Neue Presse Vom 22102021, Okt. 2021, Zugegriffen: 28. Oktober 2021. [Online]. Verfügbar unter: https://www.wiso-net.de/document/PNP__2991743112

[12] T. Kuhn, „Warum deutsche Kommunen so anfällig für Cyberattacken sind: ‚Das kannst Du doch keinem erklären'“, Wirtsch. Online 21102021, Okt. 2021, Zugegriffen: 28. Oktober 2021. [Online]. Verfügbar unter: https://www.wiso-net.de/document/WWON__WW27723492

[13] A. Schönbohm, Die Lage der IT-Sicherheit in Deutschland 2021. Bonn: BSI.

[14] A. R. Hevner, S. T. March, J. Park, und S. Ram, „Design Science in Information Systems Research“, MIS Q., Bd. 28, Nr. 1, S. 75–105, 2004, doi: 10.2307/25148625.

[15] F. Moses, K. Sandkuhl, und T. Kemmerich, „Empirical Study on the State of Practice of Information Securty Maturity Management in Local Government.“, in Human Centred Intelligent Systems 2022 - Proceeding of the 15th International Conference on Human Centred Intelligent Systems (KES-HCIS-22). Smart Innovation, Systems and Technologies., A. Zimmermann, Hrsg. Springer. Accepted for publication. To appear June 2022., 2022.

[16] R. K. Yin, „The Case Study Crisis: Some Answers“, Adm. Sci. Q., Bd. 26, Nr. 1, S. 58, März 1981, doi: 10.2307/2392599.

[17] K. M. Eisenhardt, „Building Theories from Case Study Research“, Acad. Manage. Rev., Bd. 14, Nr. 4, S. 532–550, Okt. 1989, doi: 10.5465/amr.1989.4308385.

[18] T. Wilde und T. Hess, „Methodenspektrum der Wirtschaftsinformatik: Über-blick und Portfoliobildung“.

[19] P. Schubert und K. Bhaskaran, „The eXperience Methodology for Writing IS Case Studies“, AMCIS 2007 Proc., S. 16, 2007.

[20] A. Weber u. a., „Sichere IT ohne Schwachstellen und Hintertüren“, TATuP - Z. Für Tech. Theor. Prax., Bd. 29, Nr. 1, S. 30–36, Apr. 2020, doi: 10.14512/tatup.29.1.30.

[21] K. Weber, M. Christen, und D. Herrmann, „Bedrohung, Verwundbarkeit, Werte und Schaden: Cyberattacken und Cybersicherheit als Thema der Technikfolgenabschätzung“, TATuP - Z. Für Tech. Theor. Prax., Bd. 29, Nr. 1, S. 11–15, Apr. 2020, doi: 10.14512/tatup.29.1.11.

[22] W. Aman und J. A. Shukaili, „A Classification of Essential Factors for the Development and Implementation of Cyber Security Strategy in Public Sec-tor Organizations“, Int. J. Adv. Comput. Sci. Appl., Bd. 12, Nr. 8, 2021, doi: 10.14569/IJACSA.2021.0120820.

[23] S. U. Ahmad, S. Kashyap, S. D. Shetty, und N. Sood, „Cybersecurity During COVID-19“, in Information and Communication Technology for Competitive Strategies (ICTCS 2020), Bd. 191, A. Joshi, M. Mahmud, R. G. Ragel, und N. V. Thakur, Hrsg. Singapore: Springer Singapore, 2022, S. 1045–1056. doi: 10.1007/978-981-16-0739-4_96.

[24] S. Alagarsamy, K. Selvaraj, V. Govindaraj, A. A. Kumar, S. HariShankar, und G. L. Narasimman, „Automated Data analytics approach for examining the background economy of Cybercrime“, in 2021 Third International Con-ference on Inventive Research in Computing Applications (ICIRCA), Coim-batore, India, Sep. 2021, S. 332–336. doi: 10.1109/ICIRCA51532.2021.9544845.

[25] J. P. Kesan und L. Zhang, „An Empirical Investigation of the Relationship between Local Government Budgets, IT Expenditures, and Cyber Losses“, IEEE Trans. Emerg. Top. Comput., Bd. 9, Nr. 2, S. 582–596, Apr. 2021, doi: 10.1109/TETC.2019.2915098.

[26] K. Bouzoubaa, Y. Taher, und B. Nsiri, „Predicting DOS-DDOS Attacks: Re-view and Evaluation Study of Feature Selection Methods based on Wrapper Process“, Int. J. Adv. Comput. Sci. Appl., Bd. 12, Nr. 5, 2021, doi: 10.14569/IJACSA.2021.0120517.

[27] N. Müller, „Es muss nicht kompliziert sein“, Tech. Sicherh., Bd. 10, Nr. 03, S. 16–18, 2020, doi: 10.37544/2191-0073-2020-03-16.

[28] S. S. Alhashim und M. M. H. Rahman, „Cybersecurity Threats in Line with Awareness in Saudi Arabia“, in 2021 International Conference on Infor-mation Technology (ICIT), Amman, Jordan, Juli 2021, S. 314–319. doi: 10.1109/ICIT52682.2021.9491711.

[29] A. Andreasson, H. Artman, J. Brynielsson, und U. Franke, „A Census of Swedish Public Sector Employee Communication on Cybersecurity during the COVID-19 Pandemic“, in 2021 International Conference on Cyber Situ-ational Awareness, Data Analytics and Assessment (CyberSA), Dublin, Ire-land, Juni 2021, S. 1–8. doi: 10.1109/CyberSA52016.2021.9478241.

[30] B. W. Wirtz und J. C. Weyerer, „Cyberterrorism and Cyber Attacks in the Public Sector: How Public Administration Copes with Digital Threats“, Int. J. Public Adm., Bd. 40, Nr. 13, S. 1085–1100, Nov. 2017, doi: 10.1080/01900692.2016.1242614.

[31] S.-K. Park, S.-H. Lee, T.-Y. Kim, H.-J. Jun, und T.-S. Kim, „A performance evaluation of information security training in public sector“, J. Comput. Vi-rol. Hacking Tech., Bd. 13, Nr. 4, S. 289–296, Nov. 2017, doi: 10.1007/s11416-017-0305-7.

[32] M. A. Alharbe, „Measuring the Influence of Methods to Raise the E-Awareness of Cybersecurity for Medina Region Employees“, in Advances on Smart and Soft Computing, Bd. 1188, F. Saeed, T. Al-Hadhrami, F. Mo-hammed, und E. Mohammed, Hrsg. Singapore: Springer Singapore, 2021, S. 403–410. doi: 10.1007/978-981-15-6048-4_35.

[33] L. Coppolino, S. D’Antonio, G. Mazzeo, L. Romano, und L. Sgaglione, „How to Protect Public Administration from Cybersecurity Threats: The COMPACT Project“, in 2018 32nd International Conference on Advanced Information Networking and Applications Workshops (WAINA), Krakow, Mai 2018, S. 573–578. doi: 10.1109/WAINA.2018.00147.

[34] J. Drmola, F. Kasl, P. Loutocký, M. Mareš, T. Pitner, und J. Vostoupal, „The Matter of Cybersecurity Expert Workforce Scarcity in the Czech Republic and Its Alleviation Through the Proposed Qualifications Framework“, in The 16th International Conference on Availability, Reliability and Security, Vi-enna Austria, Aug. 2021, S. 1–6. doi: 10.1145/3465481.3469186.

[35] M. Lehto, ECCWS 2020 19th European Conference on Cyber Warfare: Warfare and Security. 2020.

[36] M. Phelps, „The role of the private sector in counter-terrorism: a scoping re-view of the literature on emergency responses to terrorism“, Secur. J., Bd. 34, Nr. 4, S. 599–620, Dez. 2021, doi: 10.1057/s41284-020-00250-6.

[37] I. Choi, J. Lee, T. Kwon, K. Kim, Y. Choi, und J. Song, „An Easy-to-use Framework to Build and Operate AI-based Intrusion Detection for In-situ Monitoring“, in 2021 16th Asia Joint Conference on Information Security (AsiaJCIS), Seoul, Korea, Republic of, Aug. 2021, S. 1–8. doi: 10.1109/AsiaJCIS53848.2021.00011.

[38] R. Dreyling, E. Jackson, und I. Pappel, „Cyber Security Risk Analysis for a Virtual Assistant G2C Digital Service Using FAIR Model“, in 2021 Eighth International Conference on eDemocracy & eGovernment (ICEDEG), Quito, Ecuador, Juli 2021, S. 33–40. doi: 10.1109/ICEDEG52154.2021.9530938.

[39] C. Mironeanu, A. Archip, C.-M. Amarandei, und M. Craus, „Experimental Cyber Attack Detection Framework“, Electronics, Bd. 10, Nr. 14, S. 1682, Juli 2021, doi: 10.3390/electronics10141682.

[40] R. Savold, N. Dagher, P. Frazier, und D. McCallam, „Architecting Cyber Defense: A Survey of the Leading Cyber Reference Architectures and Frameworks“, in 2017 IEEE 4th International Conference on Cyber Security and Cloud Computing (CSCloud), New York, NY, USA, Juni 2017, S. 127–138. doi: 10.1109/CSCloud.2017.37.

[41] L. Maglaras, G. Drivas, N. Chouliaras, E. Boiten, C. Lambrinoudakis, und S. Ioannidis, „Cybersecurity in the Era of Digital Transformation: The case of Greece“, in 2020 International Conference on Internet of Things and Intelli-gent Applications (ITIA), Zhenjiang, China, Nov. 2020, S. 1–5. doi: 10.1109/ITIA50152.2020.9312297.

[42] A. Bendiek, M. Schallbruch, und Stiftung Wissenschaft Und Politik, „Eu-rope’s third way in cyberspace: what part does the new EU Cybersecurity Act play?“, SWP Comment, 2019, doi: 10.18449/2019C52.

[43] A. A. Garba, M. M. Siraj, und S. H. Othman, „An Explanatory Review on Cybersecurity Capability Maturity Models“, Adv. Sci. Technol. Eng. Syst. J., Bd. 5, Nr. 4, S. 762–769, 2020, doi: 10.25046/aj050490.

[44] K. N. Zakaria, A. Zainal, S. H. Othman, und M. N. Kassim, „Feature Extrac-tion and Selection Method of Cyber-Attack and Threat Profiling in Cyberse-curity Audit“, in 2019 International Conference on Cybersecurity (ICoCSec), Negeri Sembilan, Malaysia, Sep. 2019, S. 1–6. doi: 10.1109/ICoCSec47621.2019.8970786.

[45] „BSI-Standard 200-1: Managementsysteme für Informationssicherheit (ISMS)“, Bundesamt für Sicherheit in der Informationstechnik. https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Grundschutz/BSI_Standards/standard_200_1.html?nn=128578 (zugegriffen 26. Februar 2022).

[46] DIN ISO/IEC 27001. DIN, 2018.

[47] R. Studier und epubli GmbH, Sozialgesetzbuch Fünftes Buch (SGB V) Ge-setzliche Krankenversicherung. 2021.

[48] P. Mayring, Qualitative Inhaltsanalyse: Grundlagen und Techniken, 12., Überarb. Aufl. Weinheim Basel: Beltz, 2015.

[49] U. Pfeiffer, „Eine starke Unternehmenskultur minimiert Cyberrisiken“, Digit. Welt, Bd. 6, Nr. 1, S. 24–27, 2022, doi: 10.1007/s42354-022-0429-x.

[50] T. Meuche, „Dilemmata und Wege zur Digitalisierung der öffentlichen Ver-waltung“, Gr. Interakt. Organ. Z. Für Angew. Organ. GIO, 2022, doi: 10.1007/s11612-021-00612-7.

[51] „BSI-Standard 200-3: Risikomanagement“, Bundesamt für Sicherheit in der Informationstechnik. https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Grundschutz/BSI_Standards/standard_200_3.html?nn=128620 (zugegriffen 26. Februar 2022).

[52] F. Moses und T. Rehbohm, „<kes> Die Zeitschrift für Informations-Sicherheit“, Nr. 1, 38. Jahrgang, 2022.