doi: 10.36689/uhk/hed/2018-01-009

Deployment of New Technologies as an Integral Part of Secure Information Systems Environment

Pavel BLAŽEK[1,2], Ondřej KREJCAR[1], Kamil KUČA[1]

[1] University of Hradec Králové, Hradec Králové, Czech Republic
{pavel.blazek,ondrej.krejcar,kamil.kuca}@uhk.cz
[2] University of Defense, Hradec Králové, Czech Republic

Abstract. A proposal of the information system is a complicated process. It has to comply with an environment, where it is to be applied, and the legislation and norms have to be taken into account. Potential security risks have a significant impact on the IS proposal itself. Besides requirements for main functional units, aspects, which could affect development, implementation and a safe routine operation, have to be taken into consideration. Application friendliness, which clearly influences a margin of safety, cannot be forgotten. The modern IS has to rely on current knowledge in the area of hardware and software and use to the utmost its potential. Present manuals and guidelines for the development of information system are either on a general level and do not affect technology development or they go into details and thus topicality of content is related to the time of its creation. This article is focused on bonds between dynamically developing areas which have a significant impact on the creation of the modern IS and its security.

Keywords: Information System, Smart Devices, IoT, Security

1 Introduction

Information systems (IS) based on information technology in the environment of computer networks brought both simplification of routine activities and availability of information between workplaces where a particular system is used [8]. Apart from original autonomous applications that cover management needs and simplification of the routine activities thanks to increasing hardware (HW) capacity and building of network infrastructure led to centralized systems the primarily benefit of which was continuity of individual modules outputs and centralization of generated and processed data storage.

Presently, the infrastructure of many companies lies not only in internal enterprise networks, it crosses their boundaries and uses dynamic services of public clouds. With price decrease, this trend is not connected with multinational and large companies only. The offer of different variants of cloud services is attractive even for many medium-sized companies. Modern SMART devices [2], which are able to supply a great deal of information from various areas of human activities, are

connected to the infrastructure of companies and their private or hybrid clouds. Understanding of production processes have changed with coming the Industry 4.0 [10] initiative. It represents maximum automation and robotization which is connected with high utilization of SMART technologies, high data flow, and data storages at the level of IT environment [23].

Technologies development brought concentration of computer capacity into Clouds which resulted in the availability of many services that could be dynamically modified in compliance with topical requirements [1]. Thus, users have had an opportunity to use just as many systems means as necessary to complete a particular task without interfering into their own information technologies (IT). The latter applies if the user uses either powerful enough private cloud or paid services of the public cloud [17]. Early experience showed that temporary use of the cloud services could provide dynamic workspace for applications beyond the functions of the used company IS. For instance, it is an effort to enable work groups from the company infrastructure a cooperation with other subjects that otherwise, thanks to the company policy, would not have access to the internal IS [20]. Unrestrained decentralization brought along complications with duplicate data processing in the traditional company IS and in the parallel system about which the IT department was not informed. A security problem regarding a possible unauthorized use of data emerged because they were not stored in the secure environment under the administration of the given organization [19].

With the access to services organization, two new concepts occurred. The first one, the Lightweight IT contains a variant which is a conceptual antipole of the traditional concept of the company IT which is the Heavyweight IT [7]. While the Lightweight IT is able to satisfy users´ needs in a short period of time with applications, which are developed for the mobile platform mainly outside the company IT department, the Heavyweight IT is centralized complex and fully based on standards, which makes it slow in response to desired changes.

2 Problem definition

It is common for both centralized and decentralized systems that the technological progress is accompanied by the risk of security incidents with different impacts on the stability of the company. Almost every new element and access to the data network results in a potential resource of a security risk for the company. Responsible persons face the task of effective security which is not easy to meet due to a dynamic variability of potential attacks which require proper evaluation. Thanks to the functional connection between these two models, the security solution has to be beyond them with the use of their potentials.

The mobile platform is formed by smart systems [2] and monitoring devices where the security measures, commonly used on the PC platform, cannot be implemented. Their protection has to be performed on to this purpose designated network elements. These devices send quite a huge amount of data to the central storages with the use of

standard or proprietary protocols [13]. The transmitted data have to be safely transferred and stored.

In the environment of decentralized systems, the users can combine work in applications needed for their professional activities and simultaneously, they can have another running program which has nothing common with their duties, but it enables to send sensitive data outside the corporate environment without their knowledge [14]. Nevertheless, there are application modules which are able to separate store data in a mobile device to private and enterprise, it is necessary to install and configure them into the private persons´ device. This step is not possible without their agreement [27].

In general, the person with authorized access to sensitive data should be considered a potential source of the threat. The proven and trained worker does not have to be pressure resistant and does not have to recognize the use of social engineering techniques. For this reason, it is necessary to take into consideration to what depth and breadth of the data structure the access permissions should be set up.

From the perspective of the company, the data have to be treated cautiously not only due to a business secret but also they have to be pursuant to laws and norms. Regarding the processing of patient information, the European Union released standards dealing with privacy and security of personal data in the Directive 95/46/EC, on the basis of which the member states amended their legislation. Subsequently, the Czech Republic Ministry of Health prepared the medical document, Regulation 98/2012 Coll. Data for research are possible to transfer after so-called deidentification [4]. Processing of personal data anticipated changes due to the implementation of the Regulation (EU) 2016/679 known as GDPR - General Data Protection Regulation [25]. This document concerns not only information technologies but also has impact on its functioning.

3 Focused areas

Besides others, IT management methodology, in which the system is studied from the perspective of IT organization in the company structure, deals with IT security in new conditions [6], [28]. Encryption is used at different levels in order to reach data protection. The crypto protection of data stored in the public cloud or encryption of the transmission channel between the source and destination of transmitted data can be concerned [3].

A process of user authentication in the system is commonly treated by verification of username and password. In modern systems especially where sensitive data are processed, it is an effort to implement a multilevel variant. A combination of password, biometrics, generated token or RFID chip can be used [12]. A security level is done by a level of knowledge about security risks [24] and loyalty of an employee – a user. Successful implementation is based on a simple and user-friendly control.

A breach of company systems security arises from the finding the loopholes. Traditional and newsworthy is the attack led by a group or by individuals in order to

breach protection and get information which can be sold on the black market or to threaten the organization with disclosing the information to the public. Different methods can be used for the attack in dependence on the target. The reason could be rapid technical development and unsuitable implementation of technologies leading some companies to a vision of gaining a competitive advantage [18]. One reason could be the onset of bring your own device (BYOD) [9] philosophy which allows users to work on their own devices in the company environment. The IT department faced the assignment to integrate tablets and smartphones into the company IT infrastructure which was often in a fundamental contradiction with the company policy [2]. The connection of mobile devices and notebooks meant the extension of existing network with wireless technologies which is accompanied by the entire readjustment of security policy.

Recently, the start of clouds has brought another problem as a result of technical progress. Company departments, without knowledge and agreement of the IT department, hired services and data spaces while fulfilling their tasks which led to the decentralization of user accounts management and data duplicity. The data decentralization itself is not a new issue emerging in providing cloud services. If the information system is considered the element that has a function to centralize data flows for more effective usage then decentralized processing is related to the beginning of IS development and to the environment where IS were not for some reason applied.

4 Information system extension

Securing information processed within a modern company infrastructure faces new challenges and it is necessary to divide it into categories so that these categories follow logically one after another. The division is as follows:

- physical security,
- users policy,
- hardware and Network stability,
- software vulnerability.

There exist, traditional, mostly autonomous solutions for them.

Within the physical security of workplaces with expensive technologies or workplaces processing sensitive data, it is necessary to implement an adequate protection focused on limiting access to these sensitive data and on monitoring the movement of persons in a given locality. The access to specified areas can be verified via electronic security system, the movement of persons can be monitored by cameras.

Users are authors and processors of data. Damages caused by laxness or by ignorance can have a fatal influence on the existence of the whole company [16]. To avoid this security gap, it is necessary to organize in accordance with the company´s

rules and policies not only introductory training while hiring new workers, but also regularly updated trainings aimed at clarifying current threats, duties during the data processing and possible impacts in case of information leak.

Every part of the company´s technological equipment including backup power supply systems, network security by current technologies and recommended procedures requires a specific protection.

A similar situation is in the software (SW) category. It concerns an antivirus protection of workstations and servers and performing a regular update of operating systems and applications.

4.1 Initial studies

As part of independent projects were realized studies in two different entities with different areas of activity. The first one was a laboratory at the Department of Toxicology, the second one the Klokočka car store. These studies were aimed at assessing the state of protection of the intellectual and physical property of the discussed subjects. Within them, selected processes and their follow-up internal regulations relating to sensitive data as well as the level of technical equipment that prevents the physical handling of data or material of entities have been investigated.

The Laboratory of the Department of Toxicology as the non-commercial subject is a part of University of Defense structure. Its environment is less structured in all explored fields and it primarily uses features of the university information system. However, its functions are focused only on organization management and do not include support modules for scientific activities. Support for research consists of separate applications installed on user workstations. Access to all department computers is secured by the login name and password. PCs connected directly to the laboratory apparats on some laboratories are password-free. The building is monitored by a security camera system. Connectivity to the Internet is through the network elements in the IT department of the University. Their configuration could not be detected in detail. Department is located in a building under the supervision of security guard agency. Movement of persons is limited by entry guard system, based on ID cards with RFID chips that are also valid for entry to other parts of the university. Admission is granted to ID cards holders of the department and to persons accompanied by them.

Klokočka car store is focused on business and service activities. The headquarters and three branches are located in different locations in Prague. A unified data network is created by using a secure Virtual Private Network (VPN) technology to allow connection for branches to the company IS. Company headquarters includes an IT center with a point of access to the Internet. Enhanced internal network protection is realized by commercial New Generation Firewall and IPS / IDS solutions. Computers involved in IS environment are situated in offices and in client centers. Diagnostic computers in the workshops are connected to the data network too. It comes from necessity of connectivity to the manufacturer's service database. Access to the IS is protected by username and password. Computers in the workshops are kept out of the information system and their security is a based on a shared password. Protection is

addressed here by the separation of the workshop zone and the public zone. Client center computers are physically at less secure location. Because they are part of the IS, not only the username and password knowledge is needed. Persons working with them are specially trained for possible risks. The entry system is based on employee ID cards. As usual it is decentralized system with its own user DB. Entry permission for individuals is defined by its work position. The company premises are monitored by a camera surveillance system.

In both cases securing of information technologies, saved data in the system and connection to the Internet were discussed, including possibilities of a remote access for external workers or business partners. The system of access to different parts of the buildings, where the above mentioned subjects have their seats, and monitoring of the movement of the workers, used systems and their adjustment were discussed as well.

Although both subjects could be understood as diametrically different, they have common global features – putting effort into continuous development, securing information and material values. On one hand, for a research laboratory, it is important to protect material and knowledge connected to a research, on the other hand, for a car store, it is important to secure know-how and information concerning financial results of its business.

4.2 Initial Security Conception

In both subjects, the concept is based on physical security and monitoring of the persons´ movement by the autonomous camera system. Entry system of authorized persons into the areas which are related to their activities is controlled by an autonomous system using identification cards. The reason is that both subjects use in their areas specific devices and equipment of a high acquisition value.

Information system for the car store was more complex than that for the laboratory, but application equipment of laboratories was closely connected to experiments which were performed here and it is unlikely that they would be fully represented in available LIMS.

The user interface for access to applications and information system is secured by verification of the logged-in user in a uniform account database with the LDAP technology which enables Single Sign-On to computer technology and applications. Event logging at workstations is set as initial, servers were adjusted according to the company´s policy.

At the car store there were the segment of workstation network and the segment of servers providing services to employees and customers separated from each other by a router with adjusted policies filtering the required service. The access to the Internet was influenced in a similar way. A commercial protection system with a high permeability was introduced here [5]. The laboratory was separated from the servers and the Internet by a router and a system based on customized open source solution [11].

The view on both the systems at the moment of solving a security incident is similar. In all the above mentioned systems it is necessary to find out a given time

interval and records connected to it. Logs of the IT system are extensive and it could not be possible to be oriented if we do not have a further tool which would be able to find events in real time and with minimum effort. It is possible to draw conclusions only after finding out the data in all the systems.

4.3 New technologies

Although IP cameras are already a commonly used technology, they have not fully replaced analogue forerunners yet. An advantage of a camera recording system is segmentation of the records into files with a fixed record length. The length is recorded into the file name according to a single code together with the date and time of the recording and the file is saved into a data storage. An important parameter for an IP camera is the resolution of its chip scan/ scan chip which significantly influence the legibility of the recorded event.

LDAP database is the place where it is possible to save not only the username and the password but also the card code and the key tag with a RFID chip [21]. The above mentioned technology can be used for multi-level authentication of the person who is trying to log into a computer, enter a building of the company or collect material from the warehouse. Card readers of electronic locks located at the doors are equipped with a network interface which enables them to be interlocked with a switchboard of the safety and attendance system through structured cabling system that means through omnipresent network cables. The switchboard is a server application collecting, saving and evaluating information from the readers.

4.4 Protected information and management system.

The connection of mentioned above technologies into the centrally controlled system and expansion of information and management system (IMS) with events audit database and with the module of audit evaluation, we acquire a significant source of information. Time sequence of records represents the basis for setting up the maintenance of database particularly its size. To achieve that, it is necessary to meet needs of both the operator and legislation mentioned in the introduction.

With the advent of Artificial intelligence technologies and their availability [15], an opportunity to implement the mentioned data collection has emerged. Algorithms similar to those which reveal anomalies in communication network devices and detect the attack on the infrastructure can cause anomalies in the behavior of individuals and prevent losses of material and intangible possessions of a particular company.

Global successful implementation is considered the interface definition between information management modules and SMART technologies [22], [26] for its easy connection with required functionalities. As far as the construction IoT technologies were mentioned above, there is an option to insert HW solution, the concentrator which would modify input data for the IS.

Evaluation of data collection available in the given system brings a lot of information inaccessible in other systems (Fig.1). A drafted workflow proposal of the

secured laboratory information management system (LIMS) may be primarily divided into three groups:

- security,
- logistics,
- management.

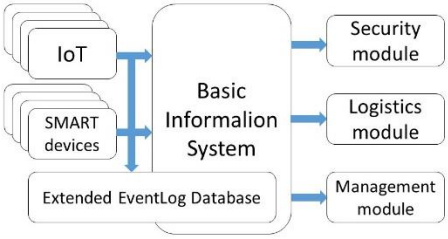

Fig. 1. Functionality extension of Basic Information System

For evaluation of security events either processed by an operator or by algorithms, there are records available from different sources with a timestamp which allow to put them in chronological order which results in a fast and easy evaluation.

For logistics, connection to the database of data from sensors brings immediate overview on material consumption and defects. Purchases may be planned and provided more easily and with early intervention on places where disrepair appears and the remedy may be made with lower money spent.

An extended system of information on persons productivity while performing their tasks is offered for the company management in overall terms the materials for the proportional burden of workers and for their evaluation.

The aim of the above mentioned solution is to effectively cover areas connected with company work activities. Specific areas of operation which involve for example monitoring and evaluation of data flow are IDS/IPS systems or New Generation Firewall /NGFW). Monitoring and evaluation of technologies and applications state are suitable to leave the System Centre for applications. It would not be suitable to bind closely the information system with platforms on which it runs independently.

5 Conclusion

Modern protected information and management systems are to be understood in a broader context than only as a support of routine activities and management. They are global immediately following units of HW and SW components and they have to comprise a functionality extended by a security audit. Its function is to create a track of events leading to the studied incident and to clarify the given event. The functionality of the model described in this article is obvious. It can be applied in

different areas of activities, wherever the data from logs and sensors linked to the given information system can be used.

Acknowledgements. This work and the contribution were also supported by project "Smart Solutions for Ubiquitous Computing Environments" FIM, University of Hradec Kralove, Czech Republic (under ID: UHK-FIM-SP-2018-2102)

References

1. Batista, N., Melício, R., Mendes, V.: Services enabler architecture for smart grid and smart living services providers under industry 4.0, Energy And Buildings, 141, 16-27 (2017), DOI:10.1016/j.enbuild.2017.02.039
2. Behan, M., Krejcar, O.: Modern smart device-based concept of sensoric networks. EURASIP Journal on Wireless Communications and Networking, pages 155 (2013), DOI: 10.1186/1687-1499-2013-155
3. Bergquist, J., Laszka, A., Sturm, M., Dubey, A.: On the Design of Communication and Transaction Anonymity in Blockchain-Based Transactive Microgrids, In Proceedings of SERIAL'17: Scalable and Resilient Infrastructures for distributed Ledgers, Las Vegas, NV, USA, December 11–15, 2017 (SERIAL'17), (2017). DOI: 10.1145/3152824.3152827
4. Blazek, P., Krenek, J., Kuca, K., Jun, D., Krejcar, O.: The system of instant access to the life biomedical data, Computational Intelligence and Informatics, 261-265 (2014), DOI: 10.1109/CINTI.2014.7028686
5. Blazek, P., Krejcar, O., Jun, D., Kuca, K.: Device security implementation model based on internet of things for a laboratory environment. IFAC-PapersOnLine, 49(25), 419-424 (2016), doi:10.1016/j.ifacol.2016.12.086
6. Brown, A. E., Grant C G.: Framing the Frameworks: A Review of IT Governance Research, Communications of the Association for Information Systems 15(38), AISeL, 695-712 (2005), ISSN: 1529-3181
7. Bygstad, B.: Generative innovation: a comparison of lightweight and heavyweight IT. Journal Of Information Technology, 32(2), 180-193 (2017). DOI:10.1057/jit.2016.15
8. Di Leva A., Laguzzi P.: Modeling Business Processes with "Building Blocks". In: Interdisciplinary Aspects of Information Systems Studies. Physica-Verlag HD, 41-46 (2008), DOI:10.1007/978-3-7908-2010-2_6
9. Eslahi, M., Naseri, M., Hashim, H., Tahir, N., Saad, E.: BYOD: Current state and security challenges, 2014 IEEE Symposium On Computer Applications And Industrial Electronics (ISCAIE), (2014), DOI:10.1109/iscaie.2014.7010235
10. Faisal, M., Katiyar, V.: Secutity Concerns in IoT Based Smart Manufacturing for Industry 4.0, International Journal of Engineering Sciences & Research Technology, 6(1), 218–221 (2017), DOI:10.5281/zenodo.245651
11. Hansen, M., Köhntopp, K., Pfitzmann, A.: The Open Source approach - opportunities and limitations with respect to security and privacy. Computers & Security, Volume 21, Issue 5, 1 October 2002, 461-471 (2002), DOI 10.1016/S0167-4048(02)00516-3
12. Ilie-Zudor, E., Kemény, Z., Blommestein, F.V., Monostori, L., Meulen, A.V.D.: A survey of applications and requirements of unique identification systems and RFID techniques, Computers in Industry, 62(3), 227-252 (2011), DOI: 10.1016/j.compind.2010.10.004
13. Katsikeas, S., Fysarakis, K., Miaoudakis, A., Van Bemten, A., Askoxylakis, I., Papaefstathiou, I., Plemenos, A.: Lightweight & secure industrial IoT communications via

the MQ telemetry transport protocol, 2017 IEEE Symposium On Computers And Communications (ISCC), DOI:10.1109/iscc.2017.8024687
14. Kaur, S.: The revolution of tablet computers and apps. IEEE Consumer Electr. Mag. (2013). doi:10.1109/MCE.2012.2223371
15. Krenek, J., Kuca, K., Blazek, P., Krejcar, O., Jun, D.: Application of Artificial Neural Networks in Condition Based Predictive Maintenance, Recent Developments In Intelligent Information And Database Systems, 75-86 (2016), DOI:10.1007/978-3-319-31277-4_7
16. Liginlal, D., Sim, I., Khansa, L.: How significant is human error as a cause of privacy breaches? An empirical study and a framework for error management, Computers & Security, 28(3-4), 215-228 (2009), DOI:10.1016/j.cose.2008.11.003
17. Maresova, P.: Decision Making Criteria for Cloud Computing Deployment. Lecture Notes In Electrical Engineering, 93-98 (2015), DOI:10.1007/978-3-662-47487-7_14
18. Pavlik, J., Komarek, A., Sobeslav, V.: Security information and event management in the cloud computing infrastructure, Computational Intelligence and Informatics, 209-214 (2014), DOI: 10.1109/CINTI.2014.7028677
19. Noor, A., Holmberg, L., Gillett, C., Grigoriadis, A.: Big Data: the challenge for small research groups in the era of cancer genomics. British Journal Of Cancer, 113(10), 1405-1412 (2015), DOI:10.1038/bjc.2015.341
20. Sobeslav, V., Maresova, P., Krejcar, O., Franca, T., Kuca, K.: Use of cloud computing in biomedicine. Journal Of Biomolecular Structure And Dynamics, 1-10 (2016), DOI:10.1080/07391102.2015.1127182
21. Sommer, A., Dukovska-Popovska, I., Steger-Jensen, K.: Agile Product Development Governance – On Governing the Emerging Scrum/Stage-Gate Hybrids. IFIP Advances In Information And Communication Technology, 184-191 (2014), DOI:10.1007/978-3-662-44739-0_23
22. Suri, K., Gaaloul, W., Cuccuru, A., Gerard, S.: Semantic Framework for Internet of Things-Aware Business Process Development, 2017 IEEE 26th International Conference on Enabling Technologies: Infrastructure for Collaborative Enterprises (WETICE). IEEE, 214-219 (2017). DOI: 10.1109/WETICE.2017.54
23. Tantik, E., Anderl, R.: Integrated Data Model and Structure for the Asset Administration Shell in Industrie 4.0, Procedia CIRP, 60, 86-91 (2017), DOI:10.1016/j.procir.2017.01.048
24. Werlinger, R., Muldner, K., Hawkey, K., Beznosov, K.: Preparation, detection, and analysis: the diagnostic work of IT security incident response, Information Management & Computer Security, 18(1), 26-42(2010), DOI:10.1108/09685221011035241
25. Wolters, P., The security of personal data under the GDPR: a harmonized duty or a shared responsibility?, International Data Privacy Law, 7(3), 165-178 (2017), DOI:10.1093/idpl/ipx008
26. Xu, L. D., He, W., Li, S.: Internet of Things in Industries: A Survey. IEEE Transactions on Industrial Informatics, 2014, 10(4), 2233-2243 (2014), DOI: 10.1109/TII.2014.2300753
27. Zhee K., Eun SK., Joo MR., Jeong J., Won D.: High-Level Design for a Secure Mobile Device Management System. In: Marinos L., Askoxylakis I. (eds): Human Aspects of Information Security, Privacy, and Trust, HAS 2013. Lecture Notes in Computer Science, 8030, 348-356 (2013), DOI: 10.1007/978-3-642-39345-7_3
28. Zhou, J.: Discussion on the Technology and Method of Computer Network Security Management. IOP Conference Series: Materials Science And Engineering, 242, 012089 (2017), DOI:10.1088/1757-899x/242/1/012089