DOI: 10.2507/29th.daaam.proceedings.161

IT EVENTS CLASSIFICATION

Lukas Kralik, David Malanik, Petr Zacek, Miroslav Matysek

This Publication has to be referred as: Kralik, L[ukas]; Malanik, D[avid]; Zacek, P[etra] & Matysek, M[iroslav] (2018). IT Events Classification, Proceedings of the 29th DAAAM International Symposium, pp.1129-1134, B. Katalinic (Ed.), Published by DAAAM International, ISBN 978-3-902734-20-4, ISSN 1726-9679, Vienna, Austria
DOI: 10.2507/29th.daaam.proceedings.161

Abstract

This paper describes essential part of project focused on developing of a web application for training and testing of IT administrators. The first half of the paper is about project and its necessity and topicality mainly in Czech Republic, however utilization of developed application will be everywhere where is needs of effective IT management. The rest of the paper is devoted to research in the area of IT events (IT service management - ITSM). There is a proposal of very simple classification of IT events, which will be used in future research and development.

Keywords: ITIL; IT events; ITSM; IT administration; IT services

1. Introduction

The quality of providing or managing of information technology (IT) services may affect the overall effectiveness of company. This caused that many processes frameworks or methodologies were created. In the most cases, it is a set of concepts, processes and procedures which allow better planning, utilization and improving IT and information systems (IS) from the perspective of IT service provider or customer. Currently, there is a really wide offer of training programs and courses with possible certification for system administrators and other employees from the field of IT. Even if the acquisition of certificate is conditioned by practical experiences then most of the trainings are theoretical. Better trainings involve case studies or practical examples. It is possible to claim there is no training program or certification which is based on practical experiences and decision abilities of participant.

Software for Training And Testing of IT Administrators (STATIA) will allow test check abilities, skills and decision in IT service management and IT security. Virtual environment will be used for testing. Whole environment will be divided into 2 parts. The first and also the largest gives a simple view on components of information system. The second part will serve as some kind of service desk where all incoming events (requests, complaints, incidents, …) will stack. User has to decide what to do on the basis of incoming events.

1.1. Similar projects

Actually, there are no similar projects at this time (in Czech Republic) which deal with practical testing in the field of IT service management and IT security. However, specialized cyber security centre – Cybernetic Polygon (Kyberneticky Polygon – KYPOL) was built in Brno under Masaryk university.

KYPOL is focused on the research, development and setting of a unique environment for threat analysis, mainly for critical infrastructure in connection with cyber security. KYPO also offer training of IT administrators but it is costly. This causes small and medium sized companies are not interested in this service.

1.2. *Necessity and topicality of project*

Information technology intersects almost all fields of human activities and it is possible to say that today business is dependent on IT. A security, which is very often underestimated, has a very important role too. Firewall and antivirus is sufficient protection in many companies.

	nr. of trainings	**CZK**	**EUR**
ITIL / ITSM	260	21356	790,26
COBIT	19	23182	857,83
ISMS	8	14925	552,29
Lean IT	2*	18156	671,85
IT security	87	38491	1424,33
IT management	225	22488	832,15

Table 1. Number of training in related areas [1], [2], [3]

There many possible trainings and courses about managing of IT but it is very often expensive [1], [2], [3] (Table I) – average pay in Czech Republic is about 29,000 Czech Koruna (CZK) [4] ,[5]. Also, the most of these trainings are very specific and focused on one area (eg. ITSM). If these trainings include some test environment, then this environment is almost same with predictable actions which may be easily learned and remembered. But in real system, security incidents and all IT events are very difficult predictable – It is nearly impossible to find what will happen in next hour. Of course, they have prepared steps to solve incident but there are many variables which may affect the evolution of an incident. IT admins have to immediately decide what to do.

1.3. Purpose and objective of this paper

The main purpose of this paper is analysis of possible IT events that are necessary for developing of testing environment. Minor objective is to find answer on the following questions:

- Is it possible to merge and classify IT events into groups?
- What is the frequency of occurrence – which IT events encounter more frequently?

Mentioned questions are crucial for building scenarios in testing environment. Testing environment has to provide scenarios that are close to the real situations. This will allow more effective training and testing of IT administrators.

2. Methodology

STATIA is based on web technologies (PHP, MySQL, HTML5, JavaScript and CSS). These selected technologies allow multiplatform availability. The only one condition is access to the Internet; however, there still possibility of local installation in isolated local network. The first necessary step was a technical specification of project, graphical design, and database structure. Also, all these components were implemented as a first. Whole application has 2 major parts – frontend and backend. Backend is designed for administration where is possible to edit testing environment such as adding new system components (computers, servers, network components …) and edit its properties. Backend also allow to add or modify tests or create own scenario. Frontend is intended for testing IT administrators or users.

Interface will be divided on console with incoming events and the major part of interface – schematic system overview. Tested user can see all system elements and their links and dependencies. This should help to fully understand the incoming event which is crucial for right decision and preparing a solution. Every device in schematic system overview will be interactive and will provide a menu with potential actions. The menu will show only actions which will be available for specific device. Choosing actions in correct order and finding problem will lead to final evaluation. Analysis and implementation of PRNG is based on previous research and projects about PRNG and also on standardized generators. This analysis has to provide important information for design of new generator with utilization of deterministic chaos [6], [7].

Final test, mainly for designed generators, will be performed according to the NIST methodology. This will be supported by entropy and probability distribution. Implementation and test will be performed in Python 3.x and then linked with web application.

2.1. Minor goals

Fulfilling main goal is conditioned by successful achieving of minor goals – millstones, which were defined as follows:

- Analysis of possibilities of actually used Pseudo-random numbers generátor (PRNG);
- Design of PRNG for the purpose of this project;
- Implementation of PRNG;
- Testing and optimization of PRNG;
- Survey about IT events;
- Classification of IT events;
- Analysis of methods for creating and modelling scenario;
- Design and creation of some scenarios;
- Technical specification;
- Graphical user interface and database design;
- Implementation of graphics and database;
- Frontend and backend development;
- Insert data;
- Testing of application and creation of documentation.

2.2. Procedures and methods

Following procedures and methods will be used for achieving of minor goals:

- Content and expert analysis of the current state of incident management in IT.
- Analysis of methods suitable for event identification
- Analysis of possible scenarios
- Analysis of pseudorandom numbers generators
- Synthesis of acquired knowledge
- Expert assessment of the suitability of the chosen method and subsequent algorithm correction
- Design and development of SW tool – applications [8], [9], [10], [11].

Content and expert analysis of the current state of incident management in IT is the most important part for the purpose of this paper because it covers survey about IT events and their classification.

2.3. Survey about IT events

Survey contains questionnaires and mainly reviews with IT managers and specialist from all types of companies. The essential purpose of questionnaires was to prove or disprove findings from reviews. First set of IT events contained 34 events and was based on reviews. All events which had more than 5 responses were taken into the account (appendix Table II - IV.). This set was transformed into questionnaires which were disseminated via email, social networks or in printed form.

3. IT Events

Fully understanding of IT events is necessary for effective IT administration. IT event has many different definitions. One of them is in ITIL1 which define IT event as a change of state which has a significant impact on IT administration and its operation. In other words, it is an alert or report created by service, some kind of monitoring tool and item or even by user [12], [13], [14], [15], [16]. With little exaggeration, it is possible to claim that IT event is everything that affect (positively or negatively) quality level of provided IT services. Thanks to these facts, there no general classification of IT events and every company or every IT manager has their own classification. The guidelines for classification of IT events should be downloaded from Internet – just Google searching find 8 related links on first page. But very often, these guidelines are related with specific company provided consultation in ITSM or ITSM tool. General classification and definitions of individual categories does not exist, even ITIL does not include this classification in its publications [12], [13], [14], [15], [16].

[1] ITIL – well-known international framework for IT service management. Its name came as an acronym for IT Infrastructure Library; however, ITIL is original and official trademark of AXELOS Limited.

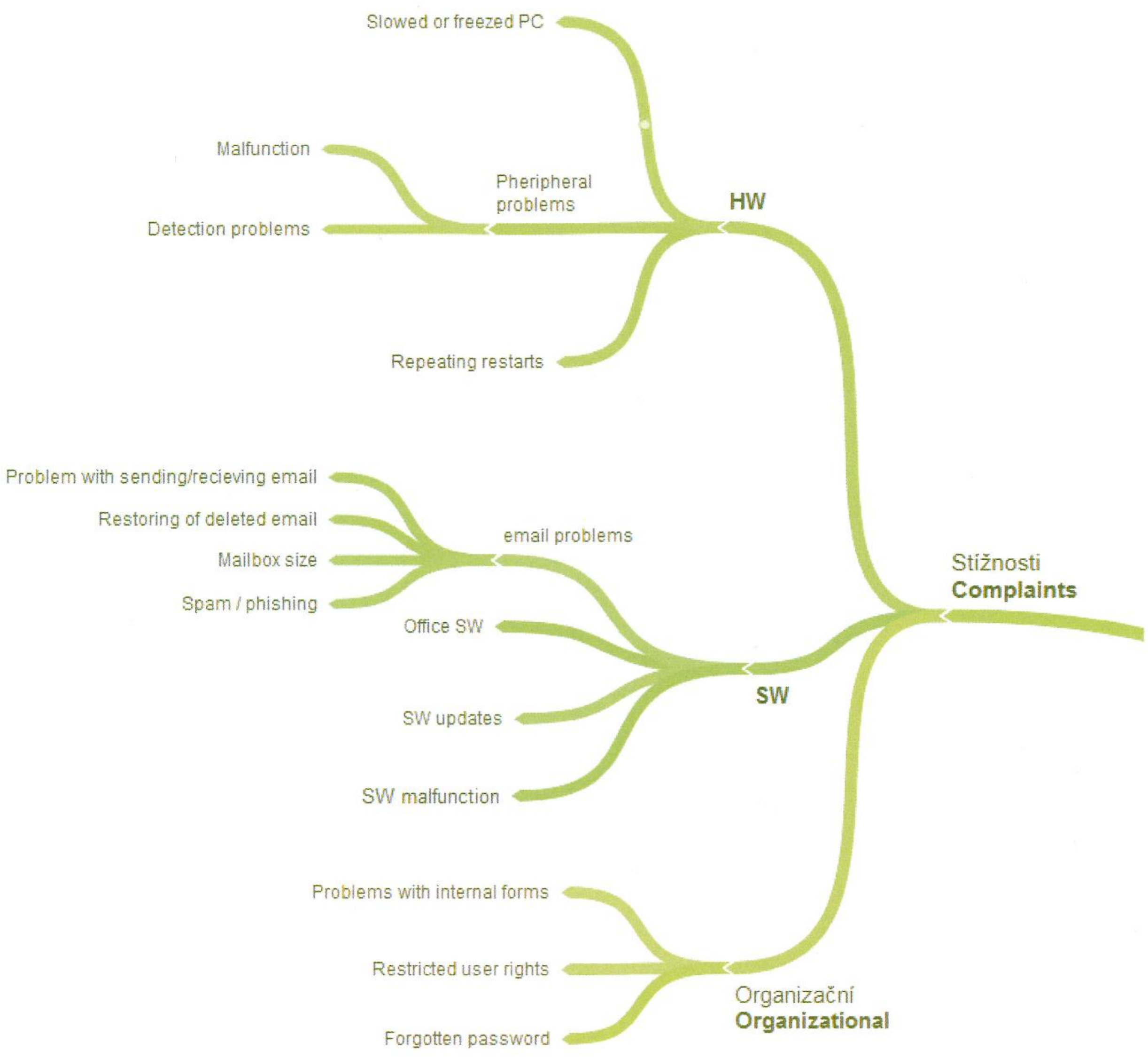

Fig. 1. Example of complaints branch

However, every guideline for classification has similar parts; also companies use some kind of classification which shows some similarity. STATIA project used this similarity in combination with results from survey about IT events to create a mind map with possible categories.

Created mind map has 4 main branches based on the source:

1. Requests
2. Compliance
3. Reports / alerts
4. Incidents

Every main branch has lower level branches (sub-categories) which lead to individual events. The example of branching is demonstrated in figure 1 where is only one branch (complaints) because whole mind map is too large and new events are still added. Branches complaints and requests have same second level, which contain software (SW) branch, hardware (HW) branch and organizational branch. What covers SW and HW branches is clear – problems with peripheral devices or problems with emails/office applications.

Organizational branch covers everything what is related with organizational structure, rights, duties and permissions in company (e.g. restricted access to directories or functions of information system). Reports / alerts branch is the simplest branch. There are outputs generated by some application or device. These outputs describe actual state of the device or system.

All these reports, alerts, warnings or errors are processed and evaluated which leads to identification of incidents. Consequently, incident branch is divided on simple incidents and important security incidents. The simple incident should be a lack of toner in printer but detection of malware is security incident.

Finally, it is possible to claim that IT events should be divided into 4 main categories. Naturally, that some events can be classified into more categories, especially there is intersection of complaints, reports and security incident because the first identification of security incident comes from ordinary user.

4. Conclusion

This paper describes the possible classification and division of IT events in information systems. This classification is made within project STATIA which main objective is to provide service for training IT administrators especially in small and medium sized companies. Thanks to targeted segment of companies, final solution must be cross-platform and available online or offline with local installation.

This may help to save money for expensive training programs from accredited companies which focus on international standards and frameworks such as ITIL, COBIT, RESILIA, etc. The future research is focused on importance, frequency and ration of IT events in mentioned categories. All necessary data are involved in questionnaires and it is continuously processed. Also, creation and design of probable scenarios will be crucial for STATIA's success.

5. Appendix

Event	**Nr. of respondents**
slow PC	7
problems with peripheral device	18
PC self-restart/reboot	13
spam/phishing	20
problems with sending/recieving email	12
mailbox size	8
problems with office SW	11
malfunctioning after update/upgrade	16
unwillingly deleted data / email	14
problems or non-understanding of IT	12
restricted rights / access	15
forgotten password	20

Table 2. Identified events (compliants)

Event	**Nr. of respondents**
data loss	19
uncompleted backup	17
damaged backup	15
encrypted data	13
low storage space	12
HW damage	16
DoS / DDoS	9
port scanning	10
SQL injection	9
phishing	17
repeated unsuccessful login attempt	18
exploitation	7
malware detection	20
unknown device in network	11
suspicious data traffic	9
nature disasters	5

Table 3. Identified events (incidents)

Event	**Nr. of respondents**
Requests	
installation of new SW	17
reinstallation of SW	17
HW upgrade	19
HW change	18
request for new HW / peripheral device	20
Reports	
device state	20
system logs	20
warnings / alerts	20
errors	20

Table 4. Identified events (request and reports)

6. Acknowledgments

This work was supported by the Ministry of Education, Youth and Sports of the Czech Republic within the National Sustainability Programme project No. LO1303 (MSMT-7778/2014) and by the European Regional Development Fund under the project CEBIA-Tech No. CZ.1.05/2.1.00/03.0089. Also supported by the research project VI20172019054 "An analytical software module for the real-time resilience evaluation from point of the converged security", supported by the Ministry of the Interior of the Czech Republic in the years 2017-2019 and by grant No. IGA/CebiaTech/2018/007 from IGA (Internal Grant Agency) of Thomas Bata University in Zlin.

7. References

[1] Czech Statistical Office, “Small and medium sized companies in Czech economy,” (2013, March). Cited February 25, 2017 [online], from https://www.czso.cz/documents/10180/20534676/116111a01.pdf/42108b35-f884-47a3-b421-f3771aa15427?version=1.0

[2] Ivitera a.s., “Edu-city.cz,” (2017), Cited February 25, 2017 [online], from http://www.skoleni-kurzy-educity.cz/kurzy

[3] Omnicom s.r.o., “Bestpractice.cz”. (2017). Cited February 25, 2017 [online], from https://www.bestpractice.cz/cs/Vzdelavani.alej

[4] D.Holy, J. Erhartova. (2017) “Wage - wage developments, average wage 2017,” kurzy.cz, Czech Republic, 2017, cited Cited February 25, 2017 [online], from http://www.kurzy.cz/makroekonomika/mzdy/

[5] Czech Statistical Office. (2017) Average wage – second quartile of 2016.. Cited February 25, 2017 [online], from https://www.czso.cz/csu/czso/cri/prumerne-mzdy-2-ctvrtleti-2016

[6] P. Zacek, R. Jasek, and D. Malanik. (2016). “Possibilities and Testing of CPRNG in Block Cipher Mode of Operation PM-DC-LM - General overview” AIP Conference Proceedings, 1738, art. no. 120029.

[7] P. Zacek, R. Jasek, and D. Malanik. (2016) “Improvement of CPRNG of the PM-DC-LM Mode and Comparison with its Previous Version,” The Tenth International Conference on Emerging Security Information, Systems and Technologies, Nice, France, p. 57-62.

[8] Kwon, J.-W., Jeong, I.C., Moon, S.-M. (2018). Lightweight migration for web applications with framework separation Software - Practice and Experience, 48 (3), pp. 621-640. DOI: 10.1002/spe.2542

[9] Wages, N.A., Petroni, G.R. (2018). A web tool for designing and conducting phase I trials using the continual reassessment method. BMC Cancer, 18 (1), art. no. 133, . DOI: 10.1186/s12885-018-4038-x

[10] Grigorescu, C.M., Moraru, S.A., Kristaly, D.M., Polexa, R. (2009) IP surveillance software system for mobile devices. Annals of DAAAM and Proceedings of the International DAAAM Symposium, pp. 1669-1670.

[11] Mahmood, K., Shevtshenko, E., Karaulova, T., Branten, E., Maleki, M. (2015). Troubleshooting process analysis and development of application for decision making enhancement, Annals of DAAAM and Proceedings of the International DAAAM Symposium, 2015-January, pp. 663-671. DOI: 10.2507/26th.daaam.proceedings.090

[12] Axelos. (2011). ITIL Continual Service Improvement, 2nd edn, TSO, London, xi, 246 pp. ISBN 236 978-0-11-331308-2. http://www.best-management-practice.com.

[13] Axelos. (2011). ITIL Service Design, 2nd edn. TSO, London, xi, 442 pp. ISBN 978-0-11-331305-1. http://www.best-management-practice.com

[14] Axelos. (2011) ITIL Service Operation, 2nd edn, TSO, London 2011, xi, 370 p. ISBN 978-0-11-331307-5. http://www.best-management-practice.com

[15] Axelos. (2011). ITIL Service Transition, 2nd edn, TSO, London, xii, 347 pp. ISBN 978-0-11-331306-8. http://www.best-management-practice.com

[16] Axelos. (2011). ITIL Service Strategy, Stationery Office, London, xii, 264 pp. ISBN 978-011-3310-456. http://www.best-management-practice.com