PRACE NAUKOWE Akademii im. Jana Długosza w Częstochowie
Technika, Informatyka, Inżynieria Bezpieczeństwa 2018, t. VI, s. 743–753

http://dx.doi.org/10.16926/tiib.2018.06.53

Justyna Żywiołek
Politechnika Częstochowska
Wydział Zarządzania
Katedra Inżynierii Produkcji i Bezpieczeństwa
al. Armii Krajowej 19 B, 42–200 Częstochowa
e-mail: justyna.zywiolek@wz.pcz.pl

ANALYSIS OF THE OCCURENCE OF INCIDENTAL EVENTS ON THE SCOPE OF INFORMATION SECURITY IN A PRODUCTION ENTERPRISE

Abstract. The article presents the structure and analysis of possible events for information security of manufacturing enterprises. The aim of the analysis is to identify incident events, their time and frequency, occurrence. This analysis includes the occurrence of notifications, threatening events, employee errors and false alarms. The conducted research also takes into account the functions performed in the enterprise. For these events, a daily distribution of events and statistical analysis of their occurrence were developed. Thanks to the analysis of the phenomena in time, enterprises can introduce actions preventing the occurrence of incidents. The conducted research has shown that employees report incidents which, in their opinion, constitute an incident, which greatly facilitates the work of the information security administrator. These events are analysed and classified accordingly. The analysis showed that most events take place between midnight and two in the morning. The conducted analysis is extended pilot studies carried out in three large enterprises from the metallurgical industry.
Keywords: analysis of phenomena in time, information security, incidents.

ANALIZA WYSTĘPOWANIA ZDARZEŃ INCYDENTALNYCH Z ZAKRESU BEZPIECZEŃSTWA INFORMACJI W PRZEDSIĘBIORSTWIE PRODUKCYJNYM

Streszczenie. W artykule przedstawiono strukturę oraz analizę możliwych zdarzeń dla bezpieczeństwa informacji przedsiębiorstw produkcyjnych. Celem prowadzonej analizy jest rozpoznanie zdarzeń incydentalnych, ich czasu i częstotliwości występowania.

Analiza ta obejmuje występowanie zgłoszeń, zdarzeń zagrażających, błędów pracowników oraz fałszywych alarmów. Prowadzone badania uwzględniają również pełnione w przedsiębiorstwie funkcje. Dla tych wydarzeń został opracowany dobowy rozkład zdarzeń oraz analiza statystyczna ich występowania. Dzięki analizie zjawisk w czasie, przedsiębiorstwa mogą wprowadzić działania zapobiegające występowaniu incydentów. Przeprowadzone badania wykazały, iż pracownicy dokonują zgłoszeń zdarzeń, które ich zdaniem stanowią o incydencie, co znacznie ułatwia pracę administratora bezpieczeństwa informacji. Zdarzenia te są analizowane i odpowiednio klasyfikowane. Analiza wykazała, iż najwięcej zdarzeń ma miejsce pomiędzy północą a drugą w nocy. Przeprowadzona analiza to poszerzone badania pilotażowe, przeprowadzone w trzech dużych przedsiębiorstwach z branży metalurgicznej.
Słowa kluczowe: analiza zjawisk w czasie, bezpieczeństwo informacji, incydenty.

Introduction

Situations threatening information security may occur at any time and in any place. This means that enterprise is a place of potential threats, activated due to the unfavourable changes in space. The purpose of this analysis is to show the periods of probability of potentially incidental events. The study was carried out on the basis of data provided by the metallurgical and multi-employer plans enterprise. The surveyed enterprises consist of at least two departments, namely steelworks and rolling mills. Emerging signals about information security threats have caused an analysis of the occurrence of events [9]. The aim of the article is to indicate the occurrence of physical and IT events that threaten the information security of enterprises. The results of such an analysis of daily distribution and indicated employee groups that expose the company to data loss allow to overcome the safety.

Information and its safety

The basis for carrying out changes in the organization is to have relevant information that is the basis for changes, their justification and a tool for process analysis, allowing to assess whether the changes were effective and effective. Information is a very important intangible resource of an organization that can be directly translated into its value [4].

Information for management allows continuous improvement of the organization and adaptation to the constantly changing environment. Its value can be judged on the basis of the decisions made [5]. The value of information for management is called its usefulness, which changes with the passage of time.

Information security in a broad sense is understood as a state free of threats, which in turn are described mainly as [6]

– providing information to unauthorized entities,
– espionage,
– diversionary or sabotage activity.

Information security is also every action, system, method that secures the resources of data collected, processed, transmitted and stored in the memory of computers and ICT networks. Therefore, information security should be understood as a resultant of physical, legal, personal and organizational security as well as ICT.

Information safety in the surveyed enterprises is threatened in a direct way by events, which gives a basis for the analysis of these events.

Occurrence of possible events

For information security, there has been created a hierarchy of events whichmayappear in the company'sboth global and internal environment. They may also threaten human, his surroundings, or even the whole company. The structure of the occurrence of particular types of events divided into months is presented in Figures 1, 2 and 3. Figure 1 describes the occurrence of events threatening information security, while Figures 2 and 3 illustrate in detail the physical and IT threats. Physical information security threats are actions that can lead to the physical disappearance of information. it is about stealing documents [7], a pen drive, a computer or a disk, as well as breaking into a room or computer. In contrast, when talking about IT threats, we are dealing with viruses, hacking and similar activities carried out using a computer [8].

Analysis of Figure 1 proves that during the holiday season and in the months of January, February and December, the occurrence of the largest number of situations threatening the security of information can be noticed. It is related to the holiday period, winter breaks and festive seasons, during which employees often replace each other without paying much attention to the information security. In the months with the lowest intensity of information security threats their number decreases at least several times. In July and August, it ranges from 20% to 25% in the studied period. When it comes to physical threat, there is a large variation in the number of events in particular months in the considered period. July, August, December, January and February are the periods of the most frequent occurrences of physical and IT threats. It is in these months that more than half (64.2%) of the total number of threats is created. The difference between the largest and the smallest number of incidental situations in the month is very large: in February it reaches 18.6%, while in March only 2.7%. Analyzing the data of the total number of events in particular months, it can be concluded that the majority of events falls on February, July and August. The most peaceful months are March, April, May.

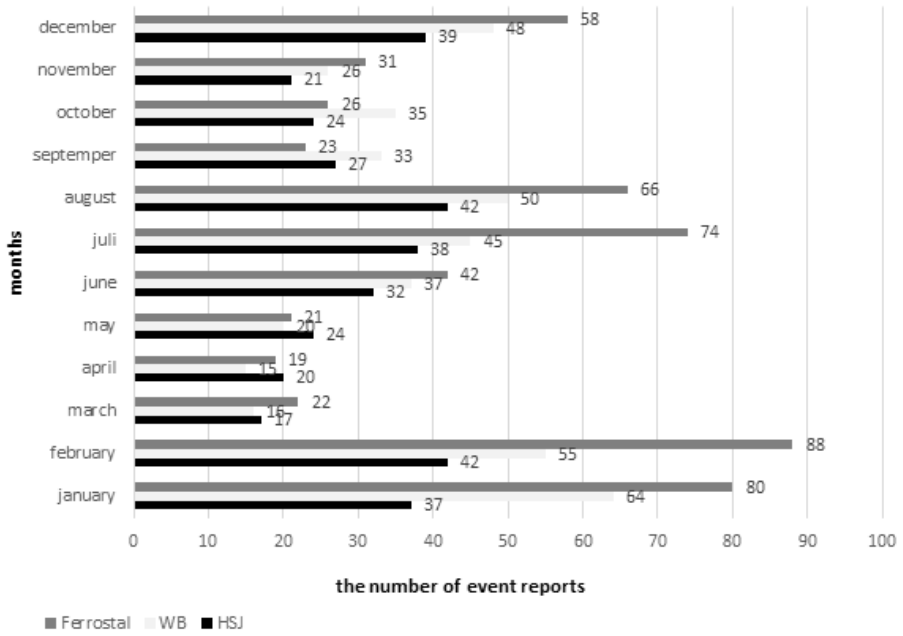

Fig. 1. Reporting events that threaten information security

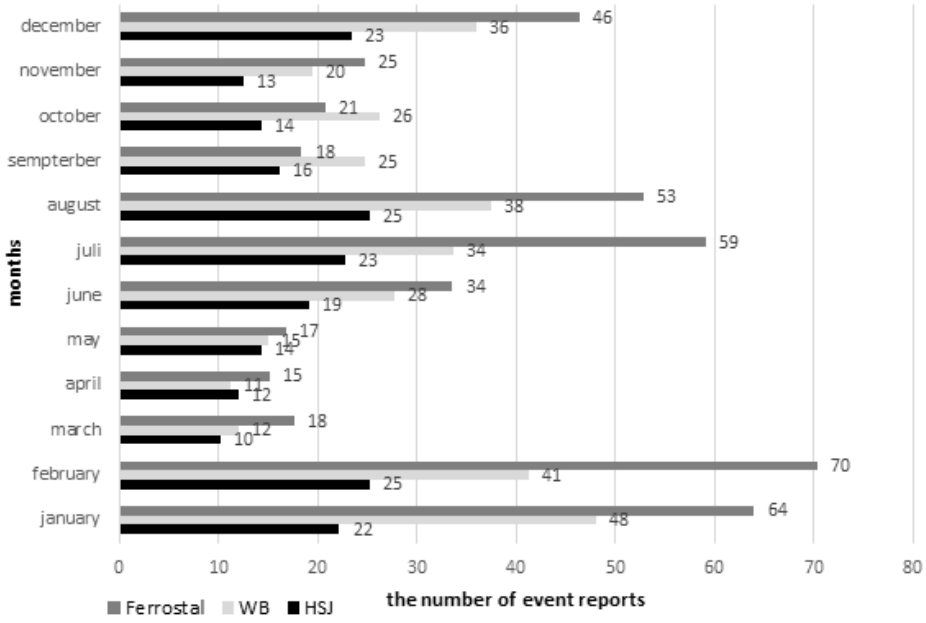

Fig. 2. Real physical threat by months

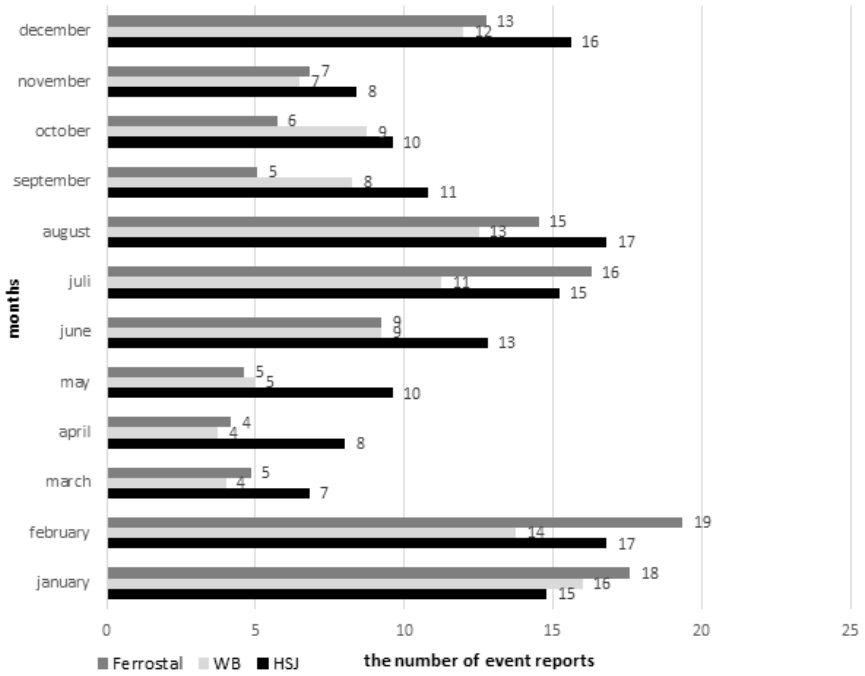

Fig. 3. Real IT threat divided into months

The period of low activity of the occurrence of events could be used for [1]:

- familiarization with possible threats;
- conducting exercises to protect from threats;
- staff training;
- IT system tests.

The diversity of the occurrence of the largest and smallest numbers of local hazards in different periods could be used to analyze events including division into days of the week and the function fulfilled in the enterprise (Figure 4).

The analysis shows that middle-level executives make the most mistakes on Fridays, as do office workers, which is caused by the five-day mode of working and fatigue at the end of it. Top executives usually make mistakes on Mondays and Fridays. The increase in the number of errors on Monday is associated with the board meetings, commonlycarried on this day of the week. Additionally, the management rarely uses IT profiles requiring changing the password every 30 days, which brings problems to the management. Therefore, situations threatening the IT system are then demonstrated.

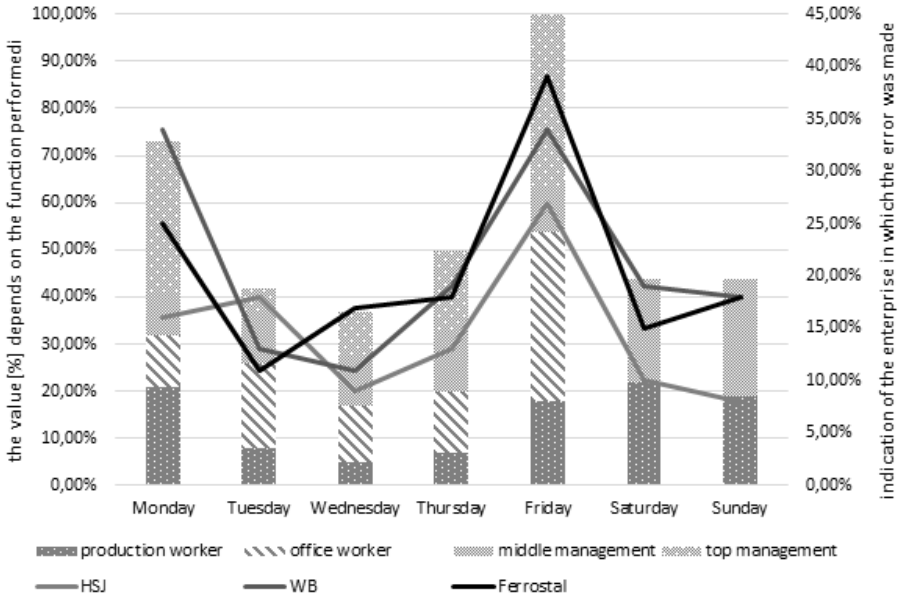

Fig. 4. Occurrence of threats on individual days including the function performed in the enterprise with an indication of the enterprise in which the error was made

Statistical analysis of the daily distribution of reports

The daily schedule of reports presented in Table 1 and Figure 5 may help in planning the activities of the examined enterprise and in preventive activities.

Table 1. The daily distribution of applications for particular types of events [1]

From an hour for hours		Reporting events	Real events	Employee error	False alarm	A total of events	Participation mistakes	Participation incidents
00:00	01:00	16	1	3	12	4	75%	25%
01:00	02:00	18	1	6	11	**7**	85%	15%
02:00	03:00	4	0	2	2	2	100%	0%
03:00	04:00	3	0	1	2	1	100%	0%
04:00	05:00	1	0	0	1	**0**	0%	0%
05:00	06:00	0	0	0	0	**0**	0%	0%

From an hour for hours		Reporting events	Real events	Employee error	False alarm	A total of events	Participation mistakes	Participation incidents
06:00	07:00	0	0	0	0	**0**	0%	0%
07:00	08:00	0	0	0	0	**0**	0%	0%
08:00	09:00	4	0	2	2	2	100%	0%
09:00	10:00	3	0	1	2	1	100%	0%
10:00	11:00	0	0	0	0	**0**	0%	0%
11:00	12:00	0	0	0	0	**0**	0%	0%
12:00	13:00	0	0	0	0	**0**	0%	0%
13:00	14:00	0	0	0	0	**0**	0%	0%
14:00	15:00	9	0	0	9	**0**	0%	0%
15:00	16:00	7	1	3	3	4	75%	25%
16:00	17:00	0	0	0	0	**0**	0%	0%
17:00	18:00	0	0	0	0	**0**	0%	0%
18:00	19:00	11	2	4	5	6	67%	33%
19:00	20:00	10	1	3	6	4	75%	25%
20:00	21:00	8	0	4	4	4	100%	0%
21:00	22:00	0	0	0	0	**0**	0%	0%
22:00	23:00	0	0	0	0	**0**	0%	0%
23:00	00:00	0	0	0	0	**0**	0%	0%

In table 1,in bold,the minimum and maximum values for the selected group of events are marked. The minimum share of employee errors in all events and the minimum share of incidents in the events are marked in gray. In turn, the green colour indicates the maximum share of employee errors in all events and the maximum share of incidents in all events. Basing on Table 1, there was developed Figure 5, which shows the daily distribution of events.

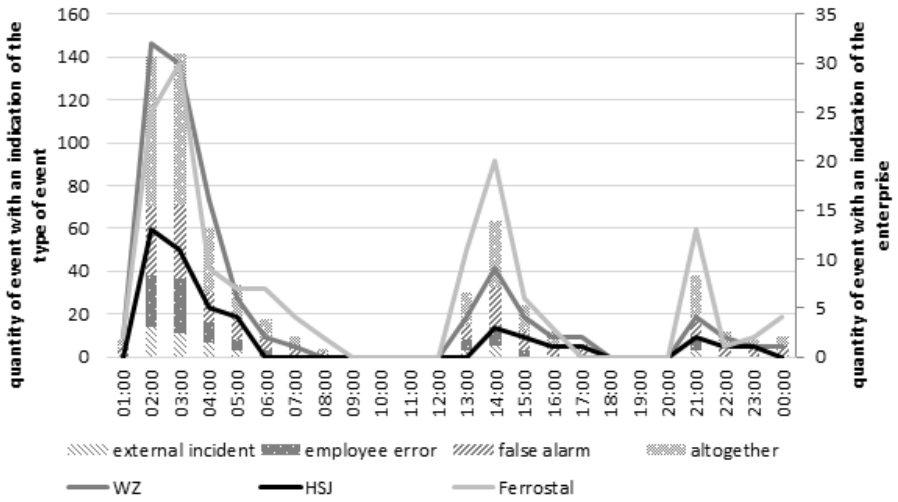

Fig. 5. Daily distribution of events for the period 2015–2017 [1]

For individual types of events, the most commonly used measures in the statistical analysis were calculated: arithmetic mean, standard deviation, coefficient of variation, quartiles and Pearson's correlation coefficient [2, 6].

The arithmetic mean $\bar{x}$ for straight lines, where the data is not ordered, is given by (1):

$$\bar{x} = \frac{1}{n}\sum_{i=1}^{n} x_i \tag{1}$$

x_i - value of the examined feature of the i-th statistical unit;
n - number of statistical units tested.

The standard deviation σ_x for a straight series is (2):

$$\sigma_x = \sqrt{\frac{1}{n}\sum_{i=1}^{n}\left(x_i - \bar{x}\right)^2} \tag{2}$$

The coefficient of variation V_x is a measure of the "quality" of the average (arithmetic), it has the form (3):

$$V_x = \frac{\sigma_x}{\bar{x}} \tag{3}$$

The calculations for the remaining possible events are described in Table 2.

Table 2. Values of calculated statistical measures used to determine the structure of the occurrence of events over time [1]

	max	**min**	**The arithmetic mean**	**The standard deviation**	**The coefficient of variation**
Reporting events	18	0	3,91	3,72	0,95
Real events	2	0	0,25	0,21	0,84
Employee error	6	0	0,58	0,46	0,79
False alarm	6	0	1,125	1,052	0,94

The values of standard deviation and variability coefficient show that the daily distribution of the number of false positives is the most diversified. Their average number over five years is 1,125 applications in one hour, with the maximum of 12 reports falling from 1:00 to 02:00 a.m., while the minimum equal to 0is from 10:00 to 02:00 p.m.. False alarm type reports have the highest correlation coefficient between their number and the total number of reports, and reach 0.94. The hours at which the most false alarms should be expected are 00:00 to 04:00. Similarly, the hours when applications will be relatively less are between 02:00 and 04:00 p.m., and 06:00 and 09:00 p.m..

By analyzing in a similar way the data on employee errors, it is possible to obtain information that the dispersion for these applications is high (coefficient of variation equal to 0.79). During the period from which the data were collected, an average of 0.58 applications per hour occurred. The most, i.e. 6 reports were recorded between 01:00 and 02:00, while for the smallest number of events reporting employee errors, these data are dispersed within 24 hours.

In turn, real events constituting threats to information security, of which 0.25 per hour on average in the analyzed period, are poorly correlated with the total number of applications.This allows to state that the more applications are made, the smaller percentage of them will be real threatening events. Analyzing the daily distribution of applications, one could conclude that the maximum number of recorded events is 2. The largest percentage was recorded between 6:00 and 8:00 p.m.. During the night hours between 00:00 and 02:00 there can also be noticed a small amount of this type of events. In other hours, events threatening information security are not noticed.

Summary

The analysis indicates that the majority of events threatening the information security of the examined enterprise occurs in January, February and during the holiday period. The information about physical IT events,with the highest frequency of such events, occurs in a similar period as general occurrences. For employee errors and false alarms, a daily distribution of events was also performed. This distributionindicated that the occurrence of these events intensifies especially during the night shift. Statistical analysis was also carried out for individual types of events. Maximum occurrence of real events, employee errors and false alarms appears between 00:00 and 02:00, whereas the minimum depends on the type of the event. The distribution of events,which include division into days of the week and the function performed in the enterprise, indicates that office employees, middle and senior managers make mistakes in a similar period of time. On the other hand, production workers commit a similar number of errors throughout the week.

Literature

[1] Grodzki G., Piech H., *Audit Expert System of Communication Security Assessment, Procedia Computer* Science, 2017.
[2] Jóźwiak J., Podgórski J., *Statystyka od podstaw*, PWE, Warszawa 2006.
[3] Liderman K*., Bezpieczeństwo informacyjne*, PWN, 2012, Warszawa.
[4] Pawełoszek I., *Semantic Organization of Information Resources for Supporting the Work of Academic Staff*, Annals of Computer Science and Information Systems, 2014.
[5] Szymonik A., *Logistyka w bezpieczeństwie*, Difin, Warszawa, 2010.
[6] Wołowski F., Zawiła-Niedźwiecki J., *Bezpieczeństwo systemów informacyjnych. Praktyczny przewodnik zgodny z normami polskimi i międzynarodowymi*, edu-Libri, 2015, Warszawa.
[7] Zou P., Lun P., Cipolla D., Mohamed S., *Cloud-based safety information and communication system in infrastructure construction*, Safety Science, Volume 98, October 2017.
[8] Żywiołek J*., Międzyorganizacyjna wymiana informacji jako element zagrożenia bezpieczeństwa informacji* [w:] Systemy bezpieczeństwa w podmiotach gospodarczych (red.) Klimecka-Tatar Dorota, Pacana Andrzej, Oficyna Wydawnicza Stowarzyszenia Menedżerów Jakości i Produkcji, Częstochowa, 2016.

[9] Żywiołek J., *Zarządzanie wiedzą o systemie bezpieczeństwa i higieny pracy w przedsiębiorstwie*, [w:] Światowy Dzień Bezpieczeństwa i Ochrony Zdrowia w Pracy 2017 (red.) Ulewicz Robert, Żywiołek Justyna, Częstochowa, 2017.