Imed El FRAY

West Pomeranian University of Technology

A new model of a system to monitor the activity of employees in the organization in accordance with ISO/IEC 27001 requirements

***Abstract**. The proposed model of the system to monitor the activity of employees focused on creating a safe and stable solution, which, together with the monitoring process, is not overloading the observed device. This model complements the organization's security policy requirements in accordance with ISO/IEC 27001 standard. It is based on known and proven technology using the advantages of similar solutions, domestic and foreign, while eliminating their drawbacks. The study showed that the proposed model provides a wide range of useful functionality for a potential supervisor in dynamically changing environment of the observed machine.*

Streszczenie.** Zaproponowany model systemu monitorowania czynności pracowników skupia się na stworzeniu bezpiecznego i stabilnego rozwiązania, które nie obciąża obserwowanej maszyny. Model ten jest uzupełnieniem wymagań polityki bezpieczeństwa organizacji zgodnie z ISO/IEC 27001. Opiera się on na znanych i sprawdzonych technologiach, wykorzystujących zalety podobnych rozwiązań krajowych i zagranicznych, jednocześnie eliminując ich wady. Przeprowadzone badania wykazały iż proponowany model zapewnia szeroki wachlarz pożytecznych dla potencjalnego nadzorcy funkcjonalności w zmieniającym się otoczeniu. **Model systemu monitorowania czynności pracowników

Keywords: information system security, monitoring system, monitoring employee activity.
Słowa kluczowe: bezpieczeństwo systemów teleinformatycznych, system monitorowania, monitoring aktywności pracowników.

Introduction

The widespread use of IT infrastructure in organizations has sped up significantly and facilitated the behavioral processes on the one hand, while on the other managers and leaders discern the increasing number of various threats [1, 2, 3, 4 and 5]. One of such important challenges in the process of information risk management is to control and supervise of employees that use the infrastructure of the workplace [6]. The competition on the market, the pursuit of success, the inclination to make a quick profit or - in extreme situations - of business intelligence activities has led to the increased need to look for the opportunities to monitor the usage of computers in companies in accordance with their intended use. The undertaken measures need to prevent such use of the corporate IT infrastructure that violates the basic values resulting from the culture of the organization, its objectives, strategies and safety [7].

The purpose of this article is to propose a new monitoring model of a system to follow the activity of employees in the computer system while respecting the fundamental rights of the monitored ones. Such a model can complement the requirements of the information system security policy of the organization. The proposed model is an improvement (defect-free) to the existing solutions for monitoring the use of IT infrastructure by company employees.

Experimental Procedures

Legal and organizational aspects of employee activity monitoring

Computerization has introduced the major changes worldwide. One should be aware that there is a high risk to use it for improper purposes. There is an increasing number of malpractices initiated by various secret services all over the world which are leading to invigilation of citizens and other forms of surveillance [8] and, consequently, to gaining access to private data without the consent of the court [9]. In some countries, e.g. the USA or Sweden it is planned to allow officially to violate the privacy of correspondence [10], phone calls and e-mails privacy in the name of national security, without any restrictions [11].

In this paper the attention is focused on the Polish context and on the measures to be taken to eliminate safely all the possible risks (the misuse of information systems) by means of specific solutions for electronic monitoring of employees.

The Polish labor law does not clearly define rules that set out explicitly the rules for monitoring the employee activity. The Article 11 of the Labor Code imposes on an employer 'the obligation to respect the dignity of every employee' [12]. Personal interests are defined in the Article 23 of the Civil Code as relating to 'personal freedom, the freedom of conscience, of correspondence secrecy, etc.' [13]. Another important document is the Polish Constitution, Article 47 and 49, which ensures the right to legal protection of his private and family life, of his honour and good reputation and the freedom and privacy of communication.' In addition, Article 51 can also be mentioned since it states that 'every citizen has the right to disclose his/her information only to the extent that they consider appropriate (except on the basis of statute)' [14].

While analyzing the above regulations, the electronic monitoring of employees can be implemented in the company with prior notification of the employees about the introduction of relevant monitoring actions and their follow-up. The employer is requested to establish and clearly define the rules of using the Internet, the applications, e-mails and all other problematic platforms, and then to publish these regulations in the existing normative acts in the company, such as statutes, procedure rules, internal management acts, etc.

Some elements of monitoring may continue to be problematic, specifically the e-mails. The employer has the rights to monitor the employees' official correspondence only when the exact instructions of their use or total prohibition were established. The private email accounts, however, still remain problematic because they are covered by the regulations concerning the above-mentioned secret correspondence. The existing solutions which are currently used in the process of monitoring the activity of workers do not give the possibility to distinguish private e-mails from the business one, which can lead to legal consequences for the company. It is clear, that every employer wants to be sure that their valuable data will not be disclosed by private email accounts.

In accordance with Article 11, Paragraph 1 of the Law on unfair competition, the unfair competition is understood as transfer, disclosure, or use of other people's secret information, or their acquisition by an unauthorized person, if it threatens or violates the interests of entrepreneurs" [15]. As one can see here, there is a paradox here. An employer cannot control the private correspondence of their

employees, but how to recognize that the valuable company data do not get leaked?

The solution to this paradox could be to lock all providers of postal services. This is absurd and unrealistic, but only official e-mail account is the one which can be controlled. The second solution is to request from the employee that he/she voluntarily abandons private correspondence rights under their employment contract. This ensures the employer's full access rights to all e-mails sent out from the workers' computers [15].

An overview of the existing solutions to monitor employees' activity

The cultural, social, etc., changes led to increased demand for various solutions used in the process of monitoring the activity of employees in the company [16]. Currently, commercially available monitoring applications/software are divided into three categories [17]:

- server-side,
- client-side and
- client-server solutions.

The first one is primarily directed towards the monitoring of the network. All network traffic, both incoming and outgoing can easily be filtered and monitored. This allows quick and efficient response to irregularities. The advantage is that the software is in a place inaccessible for unauthorized employees – therefore it is difficult to disrupt its performance or cause the damage. The disadvantage of this solution is associated with difficulty to access the preview of vital activities of a computer user – it means that everything what the traffic analysis cannot detect and show (for example, the misuse of proprietary software or copying the confidential company information and passing it to the media, etc...).

The second approach involves installing the software on any machine that is intended to be observed. This allows for accurate registration of the actions of any employee or for tracking pressed keyboard keys, for periodic screen shots and creating logs of all the operations. So created archive data are stored on the user's computer and their observation usually requires direct access to the machine, or in some cases, periodical sending the data to a specified e-mail address. Despite the above mentioned advantages, this solution is much more likely to try to interfere with the user's machines than the previous one. As the user becomes aware of the existence of the monitoring software, they may try to circumvent, disable or even remove the software from the computer. In addition, this solution is dependent on the capacity of disk space being tracked on the computer. Repeated decreasing of the disk's surface can reveal the presence of the monitoring software, and the correct operation will not be possible in the case of depletion.

The third option is a combination of the above two approaches. The first application is an *agent* that is installed on the client station which is subjected to monitoring. It aims to collect the data from the computer and then send them to the server which deals with generating the reports and gives access to logs sent out by the *agent*. This approach makes it difficult to detect *the agent* application, and thus the manipulation in logs. Additionally, any attempt to shut down or interfere with the client-side can be noted in the application on the server.

As one can see, choosing the right solution depends on the needs of the organization. All information collected during the monitoring of the organization should be stored in appropriate, safe environment. The access to them should be greatly limited, and any action within this environment should be closely and rigorously recorded [15]. Providing data (intentional, defective or as a result of an attack from the outside) to an unauthorized person would be the violation of the personal data protection and, in consequence, fatal for the company.

Conditions and results

As noted in the introduction, creating a new model of the system to be used for monitoring the activity of employees in the workplace was preceded by a survey of the existing solutions on the market. This study showed a wide variety of Polish solutions (e.g. OkoSzefa [18]) and the foreign ones (NetVizor [19] Elite Keylogger [20] StaffCop [21], etc.). In order to make an in-depth comparative analysis it was necessary to determine some criteria by which these solutions could be considered and which would help make their final ranking clear. For this purpose, the following five criteria were considered [22]:

- The architecture – in this criterion three basic properties of comparable solutions were considered. The client - server architecture, the local applications and the implementation method (the distinction between the standard Windows application, a Windows service or driver; the way how the collected data are stored was considered as the last element of the criterion).
- The invisibility of *the agent* application and the ability to complete the job - one of the most important properties of this type of application should be the inability to disable *the agent* monitoring the observation of the object involved. Invisibility is understood as the absence of files on the hard disk, of entries in the panel to add/remove program, of the start menu. It also means that there is no trace of the application from the task manager and, if the agent is implemented as a system service, the Services tab located in the tools Windows administration. In addition, because many companies have not introduced the limited user profiles, and the employees work on the accounts and possess the administrator privileges, the software is tested by closing both the limited and full rights.
- The application security - this is one of the most important criteria in the ranking. Security is understood as limiting the access of a third party to the administration console, as well as the unauthorized access in order to connect and to retrieve data from machines on the watch list. In order to check whether the data sent between the client and the server are protected against eavesdropping and how to store the logs and how they were used, the Wireshark network traffic analyzer was applied [23].
- Functionality of the application - the analysis carried out with the use of this criterion was used to present all the possibilities of individual programs.
- The computer load by the agent application – it is the most important of the above criteria. In the study of the computer load some administrative tools included in Windows measuring the performance of various machine parameters were used. The study involved four parameters: CPU load, memory usage, RAM, hard disk operations and traffic on the network interface. In order to automate and unify research activities performed on machines with various applications using Macro Recorder 4.66 Jitbit Software [24] the ten-fold macro was recorded which simulated standard office functions: working with text, web browsing, sending e-mail. To determine the reference point a computer without any software was used. Finally, the test was repeated, but this time to simulate the work of the supervisor on the other machine. Each measurement was made three times, and then averaged.

In the following Table 1 all of the criteria discussed above were collected [22]. The comparison showed both weak and strong points of the existing systems monitoring the activity of employees in the company.

Table 1. Selected research criteria for existing monitoring applications

Application Criteria	Oko Szefa (Polish appl.)	NetVizor	Elite Keylogger	StaffCop	Activity Monitor
Architecture [Type of application/ how to implement]	client-server/ win32 application or service	client-server/ win32 application	Local / driver	client-server/ service	client-server/ service
Application invisibility	- visible (can be closed by: 1 - user 2 - administrator) - Does not start in safe mode	- visible (can be closed by: 1 - administrator) - Does not start in safe mode	- visible (can be closed by: 1 - administrator with a specific knowledge) - Does not start in safe mode	- visible (can be closed by: 1 - administrator) - Does not start in safe mode	- visible (can be closed by: 1 - administrator) - Does not start in safe mode
Application security	- Administrator Console: protected - Unauthorized connection of the customer: protected - The possibility of overhearing by the network: yes - Logs secured: no - Outside the local network connection: yes	- Administrator Console: protected - Unauthorized connection of the customer: protected - The possibility of overhearing by the network: yes - Logs secured: depending on the settings - Outside the local network connection: yes	- Administrator Console: protected - Unauthorized connection of the customer: protected The possibility of overhearing by the network: 1 – content - no 2 – send - yes Logs secured: yes - Outside the local network connection: not applicable	- Administrator Console: protected - Unauthorized connection of the customer: protected - The possibility of overhearing by the network: yes - Logs secured: yes - Outside the local network connection: no	- Administrator Console: protected - Unauthorized connection of the customer: protected - The possibility of overhearing by the network: no (SSL) - Logs secured: yes - Outside the local network connection: yes
Application functionality	good	very good	sufficient	good	very good
load the computer by the agent application [without administrator intervention/ with administrator intervention]	small / small	large / very large	small / -	large / large	small / medium

As can be seen in Table 1, some of the above-described applications/software are similar to each other in some way. It results from the fact that all of them have been designed and implemented to perform similar functions. However, all these applications have some disadvantages. The first drawback is the visibility of critical applications and, in most cases, they can be closed. An employee working with the administrator privileges can switch off the application, make a prohibited abuse, and then restart it without any consequences. Another critical drawback is that none of the tested software includes tracking actions when the operating system is started in the Safe Mode. In this way a user with administrator privileges can get unattended access to the resources of both machines, as well as the resources of the Internet or a local network, which poses a serious threat and gives the opportunity to commit fraud. The next critical but less serious disadvantages are:

- significant consumption of system resources, particularly when the monitored person uses functions that require a direct connection with the observed machine. These disadvantages are especially noticeable in the applications such as: NetVizor or StaffCop. A good monitoring program should be non-invasive and transparent for the user who is using the machine,
- the lack of security logs with the users data. Files stored as opened text are significant errors in the available solution ("OkoSzefa"). Such a situation can enable the third parties to get access to the data, which may result in serious legal and financial consequences,
- In all the applications, except Activity Monitor, there are not secure communication channels. The intruder eavesdropping the network can smoothly capture logs which are transferred between the client and the server. The collected information is transmitted as an opened text.

While developing the concept of creating a new model of the system to monitor the employee activity in the computer system, some interesting solutions presented in Table 1 were used (the use of server/client architecture, protecting a console from unauthorized access, the use of SSL for communication and monitoring activities such as USB and other storage devices).

The main idea of the constructed model system is accurate and continuous monitoring of user activity in the communication system. For this purpose, the system model should be invisible and its effects in the background should not be noticeable to the observed user. According to the law, the data collected by the monitoring system should be properly secured. For this purpose, the following aspects of security information were taken into account:

- confidentiality - only authorized people would have access to the information collected.
- integrity - any attempt of unauthorized changes or interference should be detectable,
- non-repudiation – the denial of the performed actions is not possible.

To meet these requirements it is necessary to secure communication protocols as well as ensure physical security of computers and a server that stores a database.

Another important objective is to choose what information from the employee machine should be collected by the *agent*. This allows not only to customize the application to our own needs but also makes the application more universal. The collected data would be stored in the database. Temporary and log files will be hidden from the user and encrypted, not giving the possibility to be accessed and edited. When the connection to the database is denied, logs will be stored on the machine until the connection is recovered.

Below the functionality of the model of system is presented. The functionalities are divided into two main groups - monitoring and management. The first contains solely the information about the users' activities:

- Periodic screen shots - the time interval that determines the refresh rate was set. Such a function is less invasive and burdensome than the performance of the real-time preview.
- Listing of the running processes and programs - provides an easy way to view running applications, and thus to find and select those unwanted, and then adding them to a database of prohibited programs.
- The preview of visited websites - this feature not only allows to check whether the employee does not misuse the Internet during the working hours, but also allows to select a site that should be added to the proscribed list.
- Recording conversations on communicators - allows to see whether the communication channel does not leak the sensitive company data.
- Observation of outgoing/incoming e-mails - as in the case of communicators, it is a way for potential dishonest employees to leak the company's confidential data, as well as other misuses.
- Monitoring the USB activity and the file operations - observation of created, erased, modified, or copied to the flash drive files by the employee will enable the control and supervise disclosed company files.
- Time and attendance – this function allows to register the time spent in each of the applications run by the worker as well as the idle time.
- Audit installed software – to check when and what applications are installed on the observed machine.
- Monitoring of tasks assigned to printing – to check if someone is not taking away the documentation and important company information in a printed form as well as is not misusing the company equipment for private purposes.
- Print Screen Control - checking if someone does not take a screenshot unlawfully (eg. of documents protected from copying and printing). This function works in such a way that it carries its own copy of each screenshot to a temporary buffer, then sends it to the database, giving the signal to the supervisor on the incident.

The second group consists of functionality and the administrative tools. This group includes the following features:

- Generation of statistics and reports – it allows to make reports that can then be used to perform the analysis, drawing conclusions and streamline business operations,
- Starting warning on monitoring – it enables to activate an option which informs the user that their activities are monitored when the computer is shut down,
- Remote installation of agents – it allows to install a limited number of job applications through the local network,
- Sending a short text message – it allows to convey simple information message, a warning in the case of a misconduct or asks the question to the observed user,
- Downloading / uploading files - for example, it allows quick access to selected files and checks the progress of the work carried out without disturbing the user,
- Locking the computer – it allows to completely prevent the user from performing any work on the machine (for example, in case of a breach of security or misuse of company resources).
- Taking control of the machine – it allows to expropriate the user and move the computer control to the supervisor screen.

A partial model database for a better presentation of the proposed model of monitoring is shown in Figure 1.

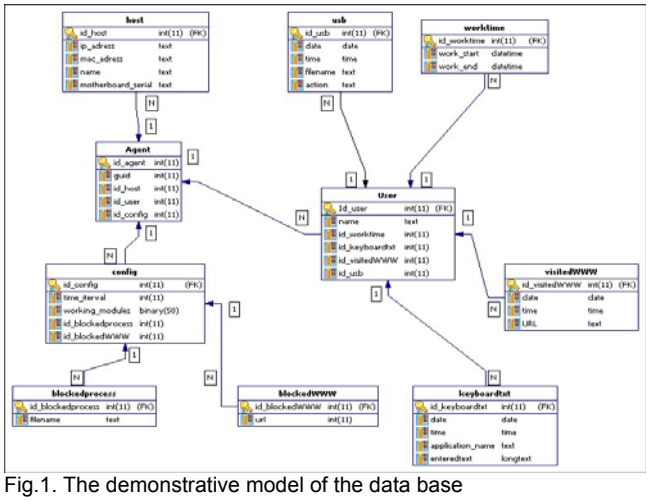

Fig.1. The demonstrative model of the data base

The so created system model for the employee monitoring was subjected to a comparative analysis with the results shown in Table 1. For the analysis in this article three criteria were taken into account: the invisibility of the agent application, the security of collected data, and computer loading under the activity of the agent (with and without the administrator's intervention).

To hide the services (the invisible agent application) the results of the Windows services [25] were used. These are related to the editing of the services base which is located in the virtual memory of the "services.exe" process which is a manager of system services. To hide the selected service, one must to find the record by name. Then, the indicators are edited on the predecessor and successor neighboring records. The following Figure 2 presents the operations to be performed, so that the service can become invisible.

During the operation, the address of hidden services is stored in the "services.exe" memory process. On this basis, according to the relevant rules, it is possible to restore the services to the list in the required situations - for example, the need to update or servicing the computer.

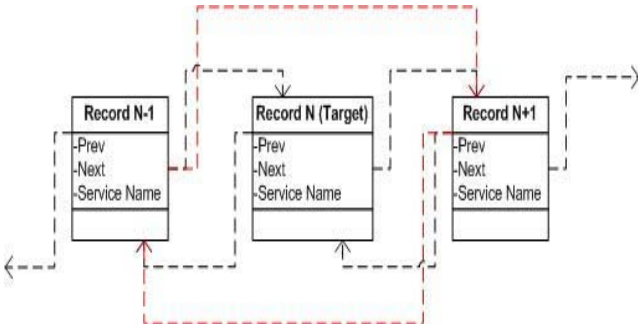

Fig.2. Method of removing services from the string

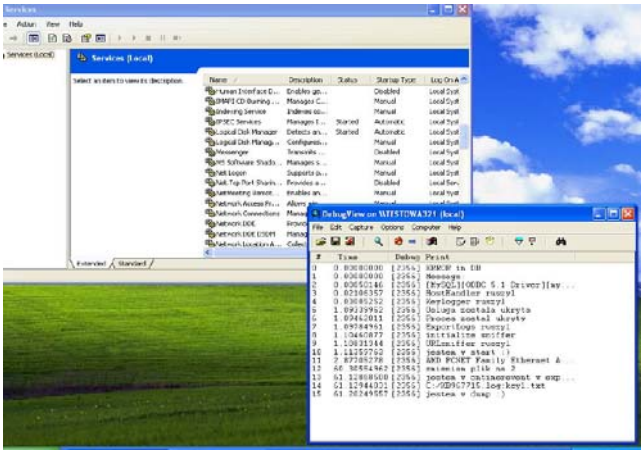

Fig.3. Invisible service “MgrService” operating in the services manager

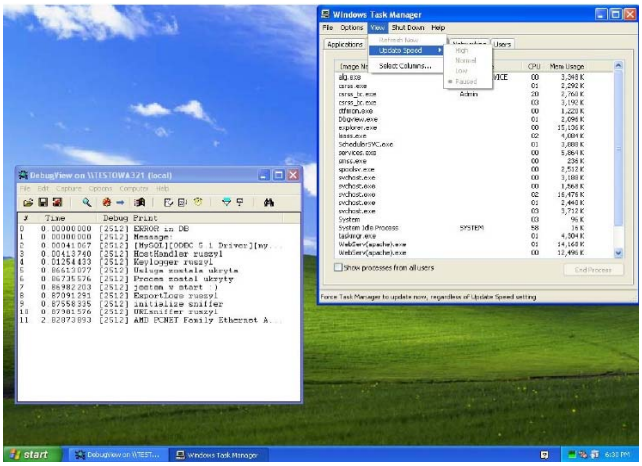

Fig.4. Invisible service operating in the "task manager"

The implementation of the modified algorithm [25] allows to hide the service when the computer is switched on. In order to enter this function a specific shortcut key should be applied. This will ensure that the application appears on the service manager list again. Figure 3 shows the evidence of invisibility service called MgrService. It shows a window manager services and DebugView application window showing the application in action.

Although the application becomes invisible from the position of service manager, it can be found in the tab of Task Manager. To achieve the complete invisibility one should remove the entry from the list of processes in the task manager where the running service applications are also included. For this purpose, the timer is implemented which checks at the specified intervals whether the window of the Task Manager is opened. If it is detected, refreshing the window is disabled and the ability to change the settings is disabled. Similar solutions are presented in [26] consisting of the appropriate manipulation of the user’s interface in such a way as to remove all entries appearing in the Task Manager tabs. As shown in Figure 4, the process of "MgrService.exe" is now visible. The proposed solution works, and most of average users will not even notice the running monitoring process.

The second criteria in the comparative analysis was to guarantee the security of data collected by the application agent. For this purpose a packet sniffer to collect the user’s input addresses was written. The packet sniffer uses the WinPcap library [27] and collects only packets with HTTP GET requests on port 80. The proposed approach significantly reduced the number of packets that should be treated in the search of URLs. The approach has the advantage of reading the history of the visited sites in file browsers. One can meet a private browser mode more and more often. If the user switches to this mode of operation, an approach based on reading the addresses from browser cache files will be ineffective. The use of a sniffer allowed to circumvent this difficulty and to collect the addresses, even if those were visited in confidence.

With the access to a variety of user-entered addresses it is possible to block the websites determined by the supervisor by placing them in the host’s file which the system is using to map the IP addresses and hostnames. The solution itself is known and can be easily overcome by the user, for example by editing the file or its removal. For this purpose the timer was used that periodically checks if the file has been removed or if the user is not trying to change the file properties. This solution is a specific kind of sentry to the host’s file. It is designed to maintain the attribute "Read Only" to prevent editing the file and in the case of removing it restores a previously created backup. The last and very important agent module which guarantees security is a module exporting data logs. It is responsible for periodica establishment of secure communication with the database and saving the local temporary logs.

The security is provided by the SSL protocol. Thanks to OpenSSL library the certificates were generated which were necessary for the agent, the console, the board and the databases. They were signed by a previously generated CA certificate. Having made the necessary configuration it was possible to establish a secure connection to a full guarantee safe browsing of the database content and to change the settings. The supervisory console developed on the model of StaffCop [21] was divided into three tabs. The first one allows to view the logs. The user selects an interesting set of information, then, if necessary, sets the appropriate filter and finally can read the data they are interested in. The second tab is the place where the supervisor inputs settings. There the time interval for the Export log module can be set and the blocked websites can be managed. The third and final tab is reserved for direct control. The access to the console is password protected and without knowing it and the correct entry procedure it is not possible to access the displayed window.

The third and final criterion in the comparative analysis was to load the computer by the agent application (with and without administrator intervention). Figures 5, 6 and 7 present the results of the experimental study which was conducted for the three solutions: OkoSzefa and StaffCop having respectively a small and large load of hard drive, memory and network interface in comparison to MgrService. The research was carried out under the same criteria as described in Chapter 3 (Section: The load of a computer with the agent application).

After the careful analysis of the values it can be stated that the OkoSzefa agent implemented as a service uses less resources and therefore causes less load on the hard drive than the agent StaffCop and the author's model MgrService, especially in the second part of the test conducted without the interference from the management. In the case of the RAM load all agents have a comparative advantage with minimal load on the agent StaffCop. The load on the network interface is much higher in the case of agents and StaffCop than the original model. The same conclusion can be drawn for testing the system administrator, especially for the hard drive and the RAM load. In turn, much more intensified use of the StaffCop interface agent and MgrService can be seen in the beginning of the test.

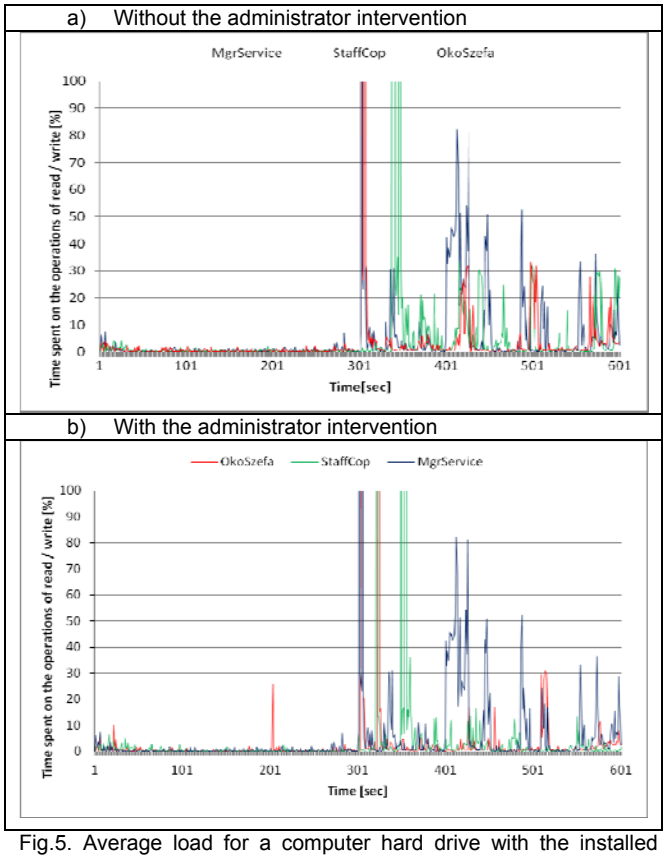

Fig.5. Average load for a computer hard drive with the installed agent

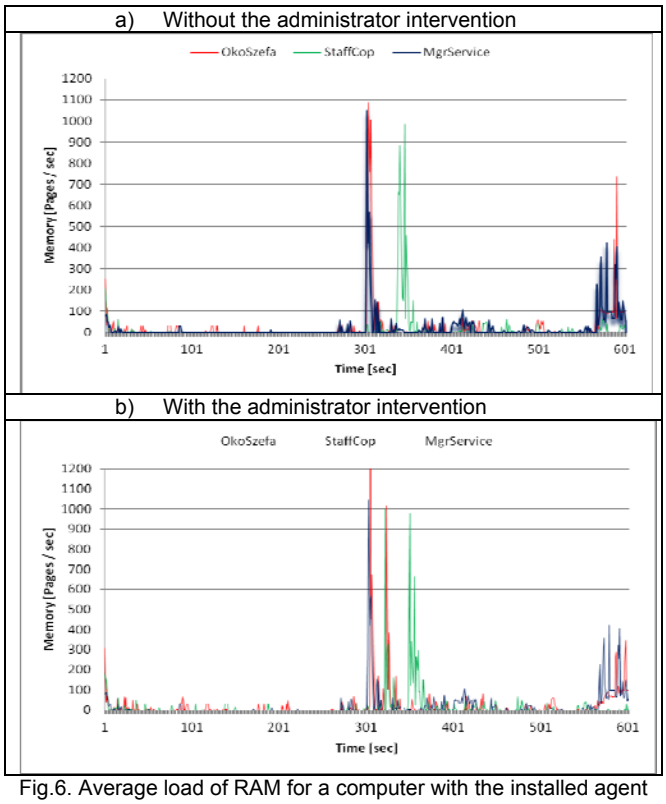

Fig.6. Average load of RAM for a computer with the installed agent

As demonstrated by the above tests, some programs occupy a lot of system resources after installing the agent. When the supervisor fetched the logs, they undertook the dialogue with the user, or just checked what they are doing at any given time, and the load increased further. It is not only uncomfortable for the worker, but, more importantly, it is also contrary to the very idea of such software, i.e. controlling the employee and not to bothering them in their duties. And the application has to be transparent and imperceptible to the user's machine. The StaffCop Agent turned out to be absorbing excessively the system resources. OkoSzefa made a very good impression, proving its work efficiency and saving the system resources. Given the pros and cons regarding the load on the system resources by our model as well as considering the innovativeness of the solution concerning the agent's invisibility as well as the design of new security measures we confirm that the proposed model of the system meets the requirements of ISO/IEC 27001 guidelines for safety management [28].

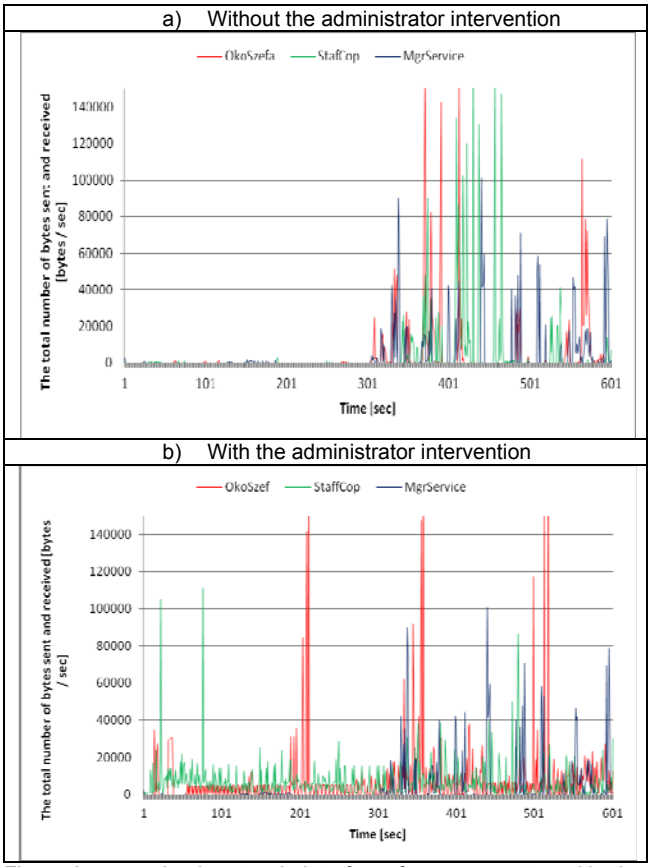

Fig.7. Average load network interface for a computer with the installed agent "

Conclusions

The proposed new system model implements all the test assumptions. It shows that the implementation of the prepared project is possible. It was also possible to overcome most of the discovered defects. First of all, the application is invisible, and thus an employee is not able to deactivate it. Due to its unique architecture, the consumption of system resources is reduced. The collected logs are temporarily hidden and additionally secured against any attempts at opening. In this way they are prevented from the risk of making the outdoor manipulation. The possibility of eavesdropping of data transported over the network was also successfully solved by means of the SSL protocol.

REFERENCES

[1] Raduan, C. R., Jegak, U., Haslinda, A., Alimin, I.I.: A Conceptual Framework of the Relationship Between Organizational Resources, Capabilities, Systems, Competitive Advantage and Performance. Research Journal of International Studies. 12(2009) 45-58

[2] Van Kleef, J.A.G., Roome, N.J.: Developing capabilities and competence for sustainable business management as innovation: a research agenda. Journal of Cleaner Production. 15(2007) 38-51
[3] Baker, W. H., Wallace, L.: Is Information Security Under Control?: Investigating Quality in Information Security Management. Security & Privacy, IEEE. 5(2007) 36 – 44
[4] Yeh, Q-J., Chang, A., J-T.: Threats and countermeasures for information system security: A cross-industry study. Information & Management. 44(2007) 480–491
[5] FENG N., XIE J. N.: Security Risk Assessment Model Based on Evidence Theory in Multi-uncertain Environment. Chinese Journal of Management **8** (2011), 614- 621
[6] Nguyen, N., Reiher, P., Kuenning, G.H.: Detecting insider threats by monitoring system call activity. Information Assurance Workshop, IEEE Systems Man and Cybernetics Society, (2003) 45-52
[7] Badr, Y.: The Integration of Corporate Security Strategies in Collaborative Business Processes. Services Computing, IEEE Transactions on 4(2011), 243 – 254
[8] Mueller R.: The Federal Bureau of Investigation invigilate American people. http://wiadomosci.gazeta.pl/Wiadomosci/1,80645,3977985.html collected on 20 April 2012 [in Polish]
[9] Kosmaty P.: The boundaries of the secret surveillance of citizens in a democratic state of law, http://www.sprp.pl/tresc/prokurator/19cf24d513ebaf153fba4e583eed547f.pdf, collected on 20 April 2012 [in Polish]
[10] Cass, R.A., Strauss P.L.: The residential signing statements controversy. heinonline.org/HOL/LandingPage?collection=journals&handle=hein.journals/wmbrts16&div=8&id=&page=, collected on 20 April 2012
[11] Falkvinge, R.: Sweden's new wiretapping law 'much worse than the Stasi'. http://www.redicecreations.com/article.php?id=4076 , collected on 20 April 2012
[12] Szewczyk, H,.: Protection of personal interest and basic forms of employees' supervision. Movement of Jurists, Economics and Sociology 3(2011) 227-240 [in Polish]
[13] Polish Civil Code. Dz. U. 1964 No 16 section 93, Act of 23 April 1964
[14] Polish Constitution. Dz. U. 1997 No 78 section 483, 2 April 1997
[15] Chakowski M., Ciszek P.: Employee Monitoring. e-Dziennik Gazeta Prawna. 214 (2005) [in Polish] http://edgp.gazetaprawna.pl/index.php?act=mprasa&sub=article&id=116584, collected on 20 April 2012
[16] Jackson, T., Dawson, R., Wilson, D.: The cost of email interruption. Journal of Systems and Information Technology. 5(2001), pp.81 - 92
[17] Weckert J.: Electronic Monitoring in the Workplace: Controversies and Solutions. Idea Group Publishing, 2005
[18] Sack, M.A.: Model of user activity supervision system in the ICT system. Master's thesis under the direction of I. El Fray (2011)
[19] http://www.okoszefa.pl/, collected on 25 February 2012.
[20] http://www.netvizor.net. collected on 15 February 2012.
[21] http://www.elite-keylogger.com, collected on 19 February 2012.
[22] http://www.staffcop.com/, collected on 24 February 2012.
[23] http://www.wireshark.org/, collected on 21 April 2012
[24] http://www.jitbit.com/macro-recorder/, collected on 21 March 2012
[25] Wineblat,E.: Service Hiding, Apriorit Inc., http://www.codeproject.com/KB/system/service-hiding.aspx, collected on 10 March 2012
[26] Sheik Abdullah: Hack Windows Task Manager. http://www.codeproject.com/KB/system/Hack_Windows_Task_Manager.aspx, collected on 10 March 2012
[27] http://www.winpcap.org/default.htm, collected on 10 March 2012
[28] ISO/IEC 27001: Information technology – Security techniques – information security management systems (2005)

***Author**: dr inż. Imed El Fray, West Pomeranian University of Technology, Faculty of Computer Science and Information Technology, Żołnierska 49, 71-210 Szczecin, Poland, E-mail: ielfray@wi.zut.edu.pl*