Asesorías y Tutorías para la Investigación Científica en la Educación Puig-Salabarría S.C.
José María Pino Suárez 400-2 esq a Lerdo de Tejada. Toluca, Estado de México. 7223898475
RFC: ATI120618V12

Revista Dilemas Contemporáneos: Educación, Política y Valores.
http://www.dilemascontemporaneoseducacionpoliticayvalores.com/
Año: VII Número: 1 Artículo no.:49 Período: 1 de septiembre al 31 de diciembre, 2019.

TÍTULO: La seguridad de las redes WI-FI en el entorno universitario.

AUTORES:

1. Ph.D. Peter Losonczi.

2. Ph.D. Martina Vackova.

3. Prof. Pavel Necas.

RESUMEN: Este artículo trata sobre el funcionamiento de las redes WiFi y las medidas de seguridad en las universidades. El artículo describe amenazas generales, puntos de partida de la operación de redes Wi-Fi en las universidades, y también los riesgos específicos para dicho entorno. Los autores presentan medidas de seguridad que representan medidas estándar y medidas que la propia operación de dichas redes ha adquirido en la práctica. El artículo también presenta consecuencias más amplias como resultado de romper las reglas en el funcionamiento de las redes Wi-Fi en las universidades. Tal hecho puede influir en los operadores de las propias redes; es decir, en una universidad particular.

PALABRAS CLAVES: seguridad, WiFi, red inalámbrica, universidad.

TITLE: The Security of the WI-FI Networks in University Environment.

AUTHORS:

1. Ph.D. Peter Losonczi.

2. Ph.D. Martina Vackova.

3. Prof. Pavel Necas.

ABSTRACT: This article deals with the operating of the WiFi networks and the security measures taken at universities. Following the preliminary presenting of the general threats the article describes the starting-points of the operating the Wi-Fi networks at universities, and also specific risks for such an environment. The risks are based on the autors´ knowing the issue and their research in this field. Next, the authors present security measures representing the so called standard measures, and measures that have been recquired by the operating itself of such networks in practice. The article also presents wider consequenses as a result of breaking the rules in operating the Wi-Fi networks at universities. Such a fact can influence operators of the networks themselves, namely particular universitie.

KEY WORDS: security, WiFi, wireles network, university.

INTRODUCTION.

At the present time, wireless networks are a very favourite technology, primarily thanks to the simplicity of connecting a various kind of equipment to the networks.

Towns and cities where people live, their places of work, their homes, hospitals, shopping centres, trains, universities and other public and private buildings are equipped with a Wi-Fi connection (Redondi *at al.*, 2016). However, the simplicity of the Wi-Fi connection is at the same time a disadvantage, namely from a security point of view.

In case of the classic LAN network, eventual attackers of the networks and followers of certain communications would have to gain a physical connection to a transmission medium (ethernet cable), in case of the wireless networks attackers just have to approach within a signal (several metres) to catch a communication (a specialized aerial necessitates more than 10 m).

There are several methods to secure the Wi-Fi networks that have been developed to remove week points of the networks, and each method provides a different level of security. The most frequent threats of the wireless networks in general include: eavesdropping, sending hoaxes, repeating some messages, easy and unlawful access to the networks and their services, inaccessibility to the networks through their interrupting, simplicity of pretending to be somebody else.

The simplicity of configurating the access to the networks through the Wi-Fi technologies is balanced by a risk of security incidents. The unsecured wireless networks have a disadvantage against other types of the networks. In principle people from the environment of a wireless router can have an access to the signal even without the owner´s knowing about it . In this way network communications can be followed or the respektive WiFi network can be used for the purpose of attackers´ connecting to the Internet. Every fourth of the total 31 million Wi-Fi networks in the world used for online communications is unsecured and risky for the users. This follows from an anylysis of Kaspersky Lab (Kaspersky, 2016).

Security within the public Wi-Fi networks concerns not only their users but also providers as the networks can be attacked and abused by the third parties (hackers) which can harm the users. However, public networks can be abused by users themselves as well (unfair activities and practicies, and that is the reason why providers or mediaters can be aggrieved as well (Losonczi, 2017).

These days in the modern world of technologies, the issue of the security of the Wi-Fi networks is dealt with by a large number of scientific and professional theses and articles (Cheng, 2013; Sombatruang *at al*., 2016; Bednarczyk, 2016). Their authors are most frequently concerned with the security of the public Wi-Fi networks, e.g., Anastasia, A.V., at al. (2017), who were dealing with the security of the public access to the Wi-Fi networks in the streets of Moscow. In their article, these authors presented ways of how to reduce or prevent various types of threats in connection with the security of data transmitted via the wireless networks.

There is a large number of and types of data gained through eavesdripping the public Wi-Fi networks. Such information concerns, e.g. a list of the hotspots visited for the last time where smartphones have been connected within the last several days, next names and types of mobile phones used etc. Some of such data are not secured by some smart phone producers, primarily in case of the older types of smartphones. That is the reason why, it is possible to find out, e.g., what articles some users have read on the Internet, what videos they have followed, what words they have looked out though a web browser, it is also possible to follow other people´s e-mail conversation, their personal data, etc. What is more, some attackers are able on the basis of the MAC address to filter a particular equipment (Losonczi, 2017).

As mentioned at the beginning this article, it deals with the operating of the Wi-Fi networks and the security measures taken at universities. The aspects mentioned above are present in university environment as well where there are Wi-Fi networks of the hybride type, i.e., on the one hand, the networks serve for educating and doing research; on the other hand, the networks represent an access point for public. The used technical solutions and conceptions often move between the security of and the purpose of the solution.

DEVELOPMENT.

Securre operating the wi-fi networks at universities.

An inseparable part of the modern days is using the Internet connection even under university conditions. Universities themselves have created a very good basis consisting in the historical context (universities have always been a leader in the development of the computer networks in Slovakia). The SANET association dealing with the connectivity of the individual universities in Slovakia can be proud of capacities comparable to similar academic networks abroad; the capacities many times exceed even commercial practice.

Following up these facts, university students have a possibility to use the high-speed Internet connection. The developing of cable solutions is accompanied by creating wireless networks at universities. Such networks are, at the present time, being solved as a complex system enabling the connectivity to other academic systems as well. The point is mostly about tens to hundreds of access points placed within university campuses and managed by a centralised system. Such a system makes it possible for the users to be mobile within university campuses and without connection failure. This service markedly enhances students´ comfort at school but also brings some problems, such as illegal activities being committed via the Internet (breaking the copyright law, downloading or publishing unalawful contents, and other negative aspects) that are in no connection with university study. That is why it is necessary to operate such a system with carefulness, security and the need for monitoring its operation.

After revealing and subsequent solving such incidents by law enforcement bodies it is just a network provider (university) who will be interrogated for the purpose of providing detailed information in connection with the network. At the same time, a particular university is notified by authorities within the SANET association of breaking laws or rules of how to operate the academic networks. Failure of solving such a problem may result in excluding a particular university from the SANET association, and subquent disconnection from the academic SANET network.

In general, universities necessitate communicating between students and teachers via the electronic means, namely inside and outside the campus. The using of such means must follow rules and principles as described in guidlines meant for operating the network infrastructure. The guidlines describe, except technical and ethic rules, also legal rules describing the way of working with the information. Both students and teachers are obliged to follow the corresponding rules and legislation. Inspite these facts one can usually come accross using the Internet for activities colliding with human rights, personal data protection, copyright and/or criminal law. The problem of using the networks is, except the contents, often represented by quantity. i.e., the abuse of the networks for the purpose of downloading extremely large amounts of data, which often negatively influences other users´ or other equipment´s operation quality.

From the technical point of view it is necessary to operate several equipment that would monitor the networks as to the capacity and character of data being transmitted. A recommended concept of such a monitoring system contains the following:

- Network Monitoring – network monitoring in real time;
- Network Behavioral Anomaly Detection (NBAD) – detecting anomalies within the network operating system by using the NBA technology (Network Behavioral Analysis);
- Threat Analysis Tool – identifying real threats in the network infrastructure;
- Security Event and Information Management (SIEM) – the following up technology makes it possible to collect, consolidate and correlate log lists, and to report and generate security notifications.

Security measures within the wi-fi networks at universities.

Within monitoring the networks an important role is played by the Firewall software that separates outer and inner environments and is effectively adapted to the needs of universities. From the point of information protection management it is important to create tools making it possible to clearly identify equipment and (a) person/s breaking the specified rules. Reports about such bahaviour are usually followed by a diciplinary procedure or a criminal prosecution.

Based on the knowledge of the project called “Influence of the Wi-Fi security and its operation on university infrastructure“ and carried out at the University of security management in Košice the most frequented threats are represented by using the Internet for the purpose of dowloading both the contents within the copyright (audio and video materials) and/or software from the server outside the jurisdiction of a particular country.

There is a problem in using the so-called torrents and technologies similar to the closed communication where it is not possible to monitor the transmitted contents of data. A solution can be blocking the corresponding ports that, however, must not be used for the service purposes. It is necessary to stress that both the network service and monitoring technologies shall not serve for reading users´ communication, however, on the basis of data characteristics and its direction the technologies themselves can guess the data contents. What is even more common the communications (e-mail, chatting etc.) are usually encrypted through adjustment or an application.

Universities themselves block the selected portals dealing with xenophoby, pornography, violence, trafficking, racism etc. A suitable aid in carrying out such an activitiy are the mentioned tools using the regular updating of their producers, and they also complete the so-called black lists with the latest data. This automatic solution is completed with the manual adjusting of the network administrators, namely through blocking particular ports or addresses, resp. users. Part of the network adjusting consists primarily in creating the so-called virtual subnetworks (VLAN) differentieted from each other through adjustment and restrictions. A large network is divided into smaller parts that can be administered more effectively.

The security goal is primarily networks free of users´ identification and authorisation (e.g. Wi-Fi networks for guests, or PC points in university corridors or libraries etc.) that are limited in the transmission speed and providing the network communication. The same logic of the subnetworks (except cable distributors) is typical of the operating the Wi-Fi networks distributed, as necessary, from several access points or all access points (Access Point – AP) placed in the building of a particular school. The host Wi-Fi network, for example, is activated at an AP in a coffee house or a waiting hall, the teacher network is activated all over the building of a school, except boarding houses etc. From the security point of view it is necessary to have the incriminated rooms provided with a camera system for the purpose of clear identifying potential offenders, even in case of a stolen equipment or access data, or a device with a cloned MAC address (hardware identification address of a computer network equipment) etc.

In case of networks it is necessary to take into account intentional or unintentional attackers. Intentional attackers are usually represented by students trying the network resistance on the basis of their “hacker“ knowledge. Unintentional attackers can be users without knowing that their equipment is either infected (unfair activities are being carried out in the background of common operations) or their equipment does not meet standards of a telecommunication authority to operate similar equipment in the Central Europe, and therefore, interrupts the process of operating (this is unique these days).

A similar spectrum of threats can also be found in connecting unknown equipment to the network of universities. In principle it is prohibited to connect a private equipment to cable distributors or selected wireless networks. It is, at the same time, prohibited to arbitrarily transfer any equipment using a cable connection and connect such an equipment to other LAN connectors. This is necessary when following the network topology for the purpose of the network administrating. Any unknown equipment has an infection potential or is not adapted to the network operating as a result of an uninstalled compatible security tools and tools monitoring the condition of the connected equipment. Such arbitrary activities can, except prohibition as stated in the respective guidline, be prevented on more network levels (through the selection of LAN ports in switch boxes, through the DHCP server, the 802.1X protocol etc.), namely through the restrictions blocking any try of connecting an unauthorized equipment. Again, as to human inventiveness and a well known possibility of cloning MAC addresses, it is necessary to monitor more hardware parametres thanks to which computers on their LAN connector are unique.

As there are a lot of possible threats in such a public system like universities, the right network configuration, its monitoring and solving every day incidents of various character go hand in hand with following the rules of how to operate such equipment. In comparison to the networks used by companies, in case of university networks the frontier between indoor and outdoor threats is being lost, so the solution of the threats must be absolutely resistent (unfortunately from the part of employees as well). An example is represented by a metropolitan topology of the SANET network in Košice whose creators have learned their lessons from the history, so each of the connected schools can be connected to the network from two sides of the main optical branches of the network in Kosice (topolgy is circular) in order to insure the connectivity even in case of failure of one of the knots.

At the same time the SANET association monitors "behaviour" of the individual shools connected to the network, and, in case of breaking the rules concerning the contents of the transmission, the schools are notified through a warning, including providing data from the SANET association for the purpose of finding the offender. Failure to solve such a problem can result in excluding a particular school from the SANET association and its subsequent disconnection from the SANET network. The network monitoring does not end outside the school gate. In the world of facts and responsibility the academic networks necessitate a conscientious operating report and absolute following the rules as specified in the respective guidline.

CONCLUSIONS.

From the point of the Wi-Fi connection at universities, attention should be devoted to clear identifying and authorising every user of the network, which consists in registering the Wi-Fi equipment and its users. In this sense it is often thought about connecting the academic information system to the management system of the Wi-Fi networks, and about writing down such equipment directly onto the student card. In case of "anonym" network it is possible to find out only technical equipment, and maybe the access point, however it is not possible to assign such equipment to a corresponsing person. The result is that one can only write down such equipment onto the so-called "black lists". Such a solution will not limit conscientious users; however, it enables administrators to immediately identify users having unfair intentions.

It is necessary to realize that public access to the Wi-Fi networks resambles a sandpit on a playground. Sandpits also have operation conditions and duties referring to the care of sand and the structure of sandpits, however, parents are nevertherless afraid of their children, as these can discover various undesirable or health threatening objects (which often happens). A public Wi-Fi network is similar to a sandpit, i.e threats and attackers can be anywhere (Losonczi, 2017). In a metaphoric sense and from the security point of view, the academic Wi-Fi networks can be perceived as an oped door that can, however, never be closed, so it is necessary to follow who will come in and what their purpose is. From the point of possible threats is the present technical solution one of the most risky elements of the university infrastructure. Therefore, it is necessary and important to educate not only university students but also teachers in this field (Kovacova, Mesaros, 2016).

A security solution of these networks can consist in a more and more spreading participation of universities in the internationl project called GÉANT Eduroam that, except connecting the academic networks and providing many possibilities for students, deals with the security aspect of the authentification and authorisation access to the Wi-Fi network (students can get accsess to the Wi-Fi network through registrating a particular association that is, in Slovakia, represented by the SANET association). This enables students to get access to the Wi-Fi network at other universities as well, if the universities participate in the mentioned project. At the present time there are 8 such universities in Slovakia and 5 boarding houses; in the Czech Republic it is possible to be connected to the Wi-Fi network at 12 railway stations as well.

Within the trend of informatizing societies that follows the European union efforts to create, through the e-Europe projects, competitive space on our continent, the informatization is unstoppable. It is then necessary to racionalise these efforts and incorporate the knowledge potential into the projects dealing with information or cybernetic securities.

BIBLIOGRAPHIC REFERENCES.

1. Anastasia, A. V., Zareshin, S. V., Rumyantseva, I. S., & Ivanenko, V. G. (2017). Analysis of security of public access to Wi-Fi networks on moscow streets. 2017 IEEE Conference of Russian Young Researchers in Electrical and Electronic Engineering (EIConRus). doi: 10.1109/eiconrus.2017.7910505
2. Bednarczyk, M. (2017). Competition in the domain of wireless networks security. XI Conference on Reconnaissance and Electronic Warfare Systems. doi: 10.1117/12.2269300
3. Cheng, N., Wang, X. O., Cheng, W., Mohapatra, P., & Seneviratne, A. (2013). Characterizing privacy leakage of public WiFi networks for users on travel. 2013 Proceedings IEEE INFOCOM. doi: 10.1109/infcom.2013.6567086
4. Kovacova, L., & Mesaros, M. (2016). Bezpecnostne vzdelavanie v sucasnom svete globalizacie. Kosice, Slovakia: VSBM v KE.
5. Losonczi, P. (2018). PUBLIC WI-FI NETWORKS IN THE GLOBAL ENVIRONMENT AND THEIR SECURITY. In Globalization and its socio-economic consequences 2018 (pp. 2206–2213). ZIlina, Slovakia: University of Zilina.

6. Redondi, A. E., Cesana, M., Weibel, D. M., & Fitzgerald, E. (2016). Understanding the WiFi usage of university students. 2016 International Wireless Communications and Mobile Computing Conference (IWCMC). doi: 10.1109/iwcmc.2016.7577031

7. Kaspersky (2016). Research on unsecured Wi-Fi networks across the world. Retrieved from https://securelist.com/research-on-unsecured-wi-fi-networks-across-the-world/76733/

8. Sombatruang, N., Sasse, M. A., & Baddeley, M. (2016). Why do people use unsecure public wi-fi? Proceedings of the 6th Workshop on Socio-Technical Aspects in Security and Trust - STAST 16. doi: 10.1145/3046055.3046058.

DATA OF THE AUTHORS.

1. Peter Losonczi. Ph.D. Department of Cyber Security, The University of Security Management in Kosice, Slovakia. Email: peter.losonczi@vsbm.sk

2. Martina Vackova. Ph.D. Department of Humanities and Technological Sciences, The University of Security Management in Kosice, Slovakia. Email: martina.vackova@vsbm.sk

3. Pavel Necas. Ph.D. Department of Security Studies, Faculty of Political Science and International Relations, Matej Bel University in Banska Bystrica, Slovakia. Email: pavel.necas@umb.sk

RECIBIDO: 6 de agosto del 2019. **APROBADO:** 18 de agosto del 2019.