Annals of DAAAM for 2010 & Proceedings of the 21st International DAAAM Symposium, Volume 21, No. 1, ISSN 1726-9679
ISBN 978-3-901509-73-5, Editor B. Katalinic, Published by DAAAM International, Vienna, Austria, EU, 2010
Make Harmony Between Technology and Nature, and Your Mind will Fly Free as a Bird
Annals of DAAAM International

ADVANCED METHODS FOR SECURING THE INFORMATION SYSTEMS

MOTYL, I[vo]; PALKA, J[an] & PALKA, J[iri]

Abstract: *The aim of this study was to follow the security level of most commonly used information systems, discover all weak points and discover solutions for their elimination. The research of status the common information system shows uncomplimentary information. A lot of security items are disused or out of date. It is cardinal security risk for the information systems. The issue of this study was to find modern and effective items for securing the information systems.*

Key words: *security, information system, risk analysis, computer crime*

1. INTRODUCTION

The information system represents very important part of modern life in this age. The information systems are used in many organizations like public administration, industry, education and business. The increasing of security is a very important part of well functioning information system (Jasek et al., 2007). The securing of the information systems means infinite way because hackers are always one step from safety engineers. In many cases is security level of information systems on very low value. For increase of the security level was used three methods. Every method was analyzed, tested and evaluated. The research confirmed our expectations.

The further research will be focussed on possibilities of fractal geometry and artificial intelligence for diagnosis and protecting the information systems.

2. PROBLEM FORMULATION

The error-free functioning is very interesting for modern organizations and companies. If the information system of organization breaks down, organization will lose a lot of money. In many cases are information systems planned unscientifically and value of the information security is on a very low rate. Traditional securing process in the organizations is regarded as a necessary but additional part of the process. This behaviour leads to the underestimating the security hazards and leads to the ad hoc solutions (Burda, 2006).

2.1 The most common ways the securing the information systems

To verify the security policy security specialist has to make a security audit. When the organization has no security policy, it is necessary to create the security project and apply safety procedures. In the first step of creating the security rules is necessary to effectuate risk analysis. The risk analysis can detect weak points. It is very considerable step to undertaking of effective security precautions. The next profit of risk analysis is preparation of organization for inside and outside hazards. The organizations must envisage of many kinds of menaces. First kind of menaces is from outside of the organization. Second kind of menace is from the inside of the organization. We can make apportion of risks on many kinds for example:

- Intended risks (internal steal, competitive spying, DOS or DDoS attacks, etc.)
- Unconscious risks (malfunction of electronic machines, unwanted data deletion, badly configuration of systems, mistakes of employee, etc.)

2.2 Theory of risk analysis

The risk analysis is an instrument for board of management for protection of the information system investments. It is also possible to order a risk analysis from the professional company, but a lot of organizations builds own risk analysis. We can know a lot of methods how to elaborate the risk analysis. The international norm ISO/IEC TR 13335 determines four basic types how to create risk analysis.

- Basic procedure: Risk analysis in organizations is missing or results of risk analysis are underestimated. It is a solution used by small companies and firms with low financial budget for security.
- Unformed procedure: In this method all risks are viewed by the subjective knowledge of well experienced security technician. This way can be enough for basic securing, but it is unsatisfactory for full and detailed protection. But it is a good first step for detailed risk analysis.
- Detailed risk analysis: This is the widest and the most exact method of risk analysis. Detailed risk analysis is the best solution in the organizations where the highest level of security is needed. This method provides correct location of information system weak points.
- Combine procedure: This procedure contains the combination of all kinds of risk analysis types.

The risk analysis always contains four scenarios.

- Identification and asset evaluation
- Analysis of menace
- Analysis of vulnerability
- Countermeasure suggestion (Smejkal, 2009)

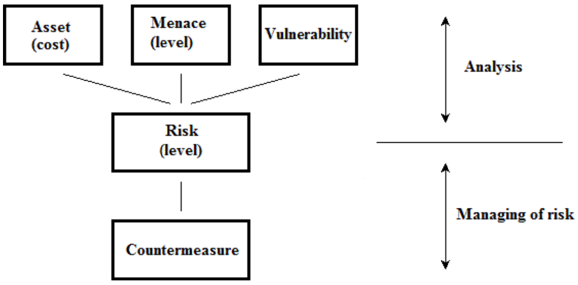

Fig. 1. Scheme of Risk analysis

3. PROBLEM SOLUTION

As we can see in many organizations and companies use only basic security elements and deficient security policies. The main problem is in misusage or bad setup of security elements like antivirus systems, firewalls, etc. For increase of security level of information systems was designed a number of innovations.

3.1 Used Honey pots

Honey pots are the security items which eliminate danger from hackers. Honey pots are systems attracting the potential attackers. For this purpose are used attractive DNS names. The main purpose of these objects is make imaginary production system or production web. The attacker is allured on this web and we can learn from the attacker's steps and make the innovation of our information system accordingly to the steps of the attacker. (Internet Systematic lab)

- High-interactive – This kind of Honey pot is realized by using any virtual machine, for example Virtual Machine, Virtual box, etc. This virtual system is unsecured. The big advantage of this solution is in large amount of information about hackers attack. For example: motivation, purpose and process of masking his steps. For evaluation of this attack is necessary to make massive analysisof attacked systems. This operation is very time-consuming. High-interactive Honey Pots can manage only very experience system administrators.

- Low-interactive – This kind of Honey pot is realized by using the special software. This software simulates any type of vulnerable service. The big advantage of this solution is the fact that we can get very easy – base information about hackers attack. (4safety)

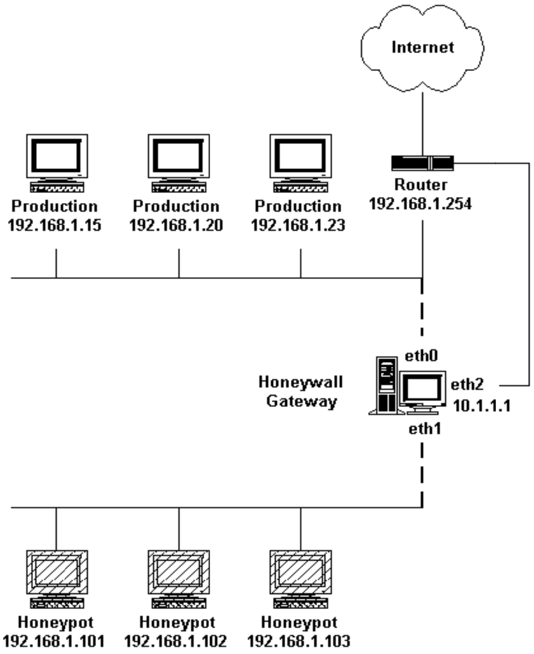

Fig. 2. Scheme of honey pots implementation

3.2 Scanner of security bugs

Scanners of security bugs are very usable instruments for every skilled administrator. These systems automatically react to vulnerable points in information system. Scanners of security bugs contain connection strings to databases which contains patches for correction codes. It is very forceful tool for securing the information systems.

The security scanners are very similar to the antivirus software. The main difference between security scanner and antivirus software is in that antivirus finds pieces of code. The main principle of the security scanner is ability to analyze computer or information system. Security scanners contain wide knowledge base about potential risks. Some of services in the information system represent weak points of security but we need to use it. The next difference between security scanner and antivirus software is in fact, that antivirus software must be installed on every computer in the computer network for successful analyze. The security scanner contains ability to analyze all computers in the computer network.

3.3 Internal advanced social engineering

Internal social engineering is one way how to quantify items of informationsystem with psychologically and scientifically procedures. One of way of internal social engineering can be verification of user attainments and loyalty in face of organization. The system administrator can send for example spam or phishing emails to users. In second step is made analysis of user steps.

On the basis of analysis interpretations are projected precautions against security holes. The main advantage of internal social engineering is low expences for testing of keeping security principles inside of information system. We don't need complexity and expensive apparatus. However for social engineering testing we need psychologically educated employee.

Internal social engineering is a very sophisticated technique for auditing of information system. Sociotechnician must be strong-minded person which can persuade to victim about company – friendly man.

4. CONCLUSION

This study was carried to evaluate the security level in the most common information systems. Our experience shows that security question is in many cases very underestimatimated. A lot of security items are disused or out of date. In the next step was designed some modern suggestions to increase of security level inside of information systems. Created innovations increased the security level of tested networks. Especially Internal advanced social angineering was evaluated as very effective method for testing psychological immunity of information systems.

The further research will be focussed on possibilites fractal geometry and artificial intelligence to diagnosis and security of information systems. This branche give a considerable potential for information system security. Hovewer we can use it in technical and nature sciences.

5. ACKNOWLEDGEMENTS

This research was supported by the Internal grant agency (IGA/31/FAI/10/D).

6. REFERENCES

Burda, K. (2006) *Bezpečnost informačních systémů*, ÚTKO FEKT VUT Brno

Jasek, R.; Dolejšová, M. & Rosman, P. (2007*) Informační technologie ve veřejné správě*, Univerzita Tomáše Bati ve Zlíně. ISBN 978-80-7318-607-4

Smejkal, V; Rais, K (2009) *Řízení rizik ve firmách a jiných organizacích,* Grada publishing. ISBN 978-80-247-3051-6

*** (2010) http://www.securityworld.cz – Securityworld, *Accessed on: 2010-5-5*

*** *(2010) http://* www.magnetosoft.com*.cz* – Magnetosoft*, Accessed on: 2010-5-5*

*** *(2010)* http://www.honeynet.gr – Internet Systematic lab*, Accessed on: 2010-5-5*

*** *(2010)* http://www.4safety.cz/text/honey - 4Safety*, Accessed on: 2010-5-5*