Myroslava VLASENKO[1]

Opiekun naukowy: Yuriy KHLAPONIN[2]

DOI: https://doi.org/10.53052/9788366249868.26

ADAPTACYJNY SYSTEM BEZPIECZEŃSTWA INFORMACJI

Streszczenie: W artykule omówiono podstawy adaptacyjnych systemów bezpieczeństwa informacji, ich zastosowanie w bezpieczeństwie informacji. Analizowane są zagadnienia organizacji przeciwdziałania atakom komputerowym na podstawie prognozowania kierunków ich rozwoju i tworzenia alternatyw dla ich przeciwdziałania. Pokazano schemat funkcjonalno-strukturalny podsystemu komputerowego przewidywania ataków.

Słowa kluczowe: ataki komputerowe, przeciwdziałanie wpływom destrukcyjnym, prognoza rozwoju wpływów destrukcyjnych, system prognozowania

ADAPTIVE INFORMATION SECURITY SYSTEM

Summary: This article discusses the basics of adaptive information security systems, their application for information security. The issues of organization of counteraction to computer attacks on the basis of forecasting of directions of their development and formation of alternatives of counteraction to them are analyzed. The functional-structural scheme of the computer attack prediction subsystem is demonstrated.

Keywords: computer attacks, counteraction to destructive influences, forecast of the development of destructive influences, forecasting system

1. Introduction

Businesses and industries are at risk with increasing cyber threats. Protecting organizational information from these cyber threats is more important than ever. A survey in the Global Risks Report by the World Economic Forum (2018) has revealed that cyberattacks are in the top ten risks both in terms of likelihood and impact. Cyberattacks are now seen as the third most likely global risk for the world

[1] Kyiv National University of Construction and Architecture, faculty of automation and information technology, specialty: 125 “Cyber Security”, bee.130974@gmail.com

[2] Doctor of Technical Sciences., Kyiv National University of Construction and Architecture, faculty of automation and information technology, y.khlaponin@gmail.com

over the next ten years. According to this study, cybersecurity risks are growing, both in their prevalence and in their disruptive potential. Cyberattacks have both short-term and long-term economic impacts on different economic agents in terms of loses and expenses. [1]

Information systems fail not only because of problems with technology used and technical incompetence of professionals administering them but also because of lack of security awarēness to the end users. The approach is adaptive in the sense that it is capable to rapidly respond to changes in business environments and changing security threats. [2]

There is nothing that is not vulnerable in computer security, everything is vulnerable! First, it is the network itself, that is, the network protocols (TCP / IP, IPX / SPX, NetBIOS / SMB) and the devices (routers, switches) that make up the network. Secondly, operating systems (Windows, UNIX, NetWare). Third, databases (Oracle, Sybase, MS SQL Server) and applications (SAP, mail and web servers, etc.) [3]

2. Brief history of adaptive security

Sun Microsystems (acquired by Oracle in 2010) coined the term “Adaptive Security Architecture” in 2008. This architecture would be able to anticipate, respond to and contain threats while reducing threat amplification, attack surface, velocity and recovery time. It was an architectural model that imitated a biological autoimmune system at a microscopic level and ecological systems on a macroscopic level.

Biological systems can respond to new conditions and adapt. They respond to threats dynamically using an innate, involuntary immune system response. Ecological systems are comprised of different components and not dependent on one single entity to survive. They are diverse and resilient.

Both systems rely on feedback to increase their ability to respond to threats. This dynamic, autonomous response found in nature is what the originators of the adaptive security model were trying to mimic. [4] [5]

3. Benefits of adaptive security

Adaptive security allows for early detection of security compromises and an automatic, autonomous response when a malicious event occurs. Other benefits of implementing an adaptive security architecture include:

- Prevent data theft and sabotage.
- Contain a threat when it occurs instantly.
- Lessen dwell time of threats.
- Recognize ongoing security breaches.
- Stop the spread of a pandemic.
- Avoid a monoculture systems environment.

There is no single system or process in adaptive security. It is a multi-level, around-the-clock monitoring system that is designed to evolve as cyber threats and attacks become more sophisticated and complex. [4]

4. Cyberspace

Cyberspace promises opportunities, but it is also grounds for power and conflict. It’s war – which is perpetuated via cybercrime with strong inclination of cybercriminals to steal and manipulate data from devices used by government agencies, society, consumers and businesses.

Such crimes may threaten a nation’s security and financial health. Like all progress - Cyberspace too, has its downside: the perverse effects manifest themselves as well, as predators immediately exploit vulnerabilities in order to gain profits, destroying or neutralizing anything that stands in the way of expanding their criminal enterprise – through cybercrime.

Figure 1 shows attack sophistication vs. intruder technical knowledge over the years. Over the years and due to the availability of highly sophisticated cyber security tools like open source BackTrack, the knowledge required to carry out a successful cyber-attack has highly reduced.

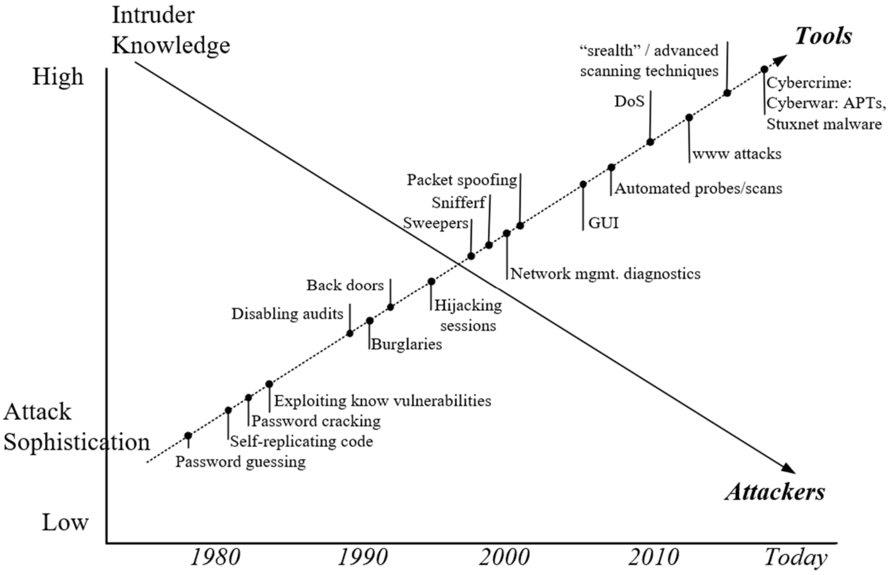

Figure 1. Attack sophistication vs. intruder technical knowledge

Some of the key advanced cyberattacks tools:

- ***Advanced Persistent Threat (APT):*** APTs are a cybercrime category directed at business and political targets by: a group, such as a foreign government, with both the capability and the intent to persistently and effectively target a specific entity.
    - *Advanced*: Criminal operators behind the threat utilize the full spectrum of computer intrusion technologies and techniques.
    - *Persistent*: Criminal operators give priority to a specific task, rather than opportunistically seeking immediate financial gain. In fact,

a "low-and-slow" approach is usually more successful – i.e., Pole Pole

- *Threat*: Implies, there is a level of coordinated human involvement in the attack, rather than a mindless and automated piece of code. i.e., the criminal operators have a specific objective and are skilled, motivated, organized and well-funded often leverage "insider threat" and "trusted connection" vectors to access and compromise targeted systems.

Hackers who employ APTs are a different breed: are a real and constant threat to the world's companies and networks, are well organized, working together as part of a professional team. Their goal, typically, is to steal valuable intellectual property, such as confidential project descriptions, contracts, and patent information. APTs breach enterprises through a wide variety of vectors, even in the presence of properly designed and maintained defense-in-depth strategies: Internet-based malware infection, Physical malware infection, and External exploitation, see Fig.2. [6]

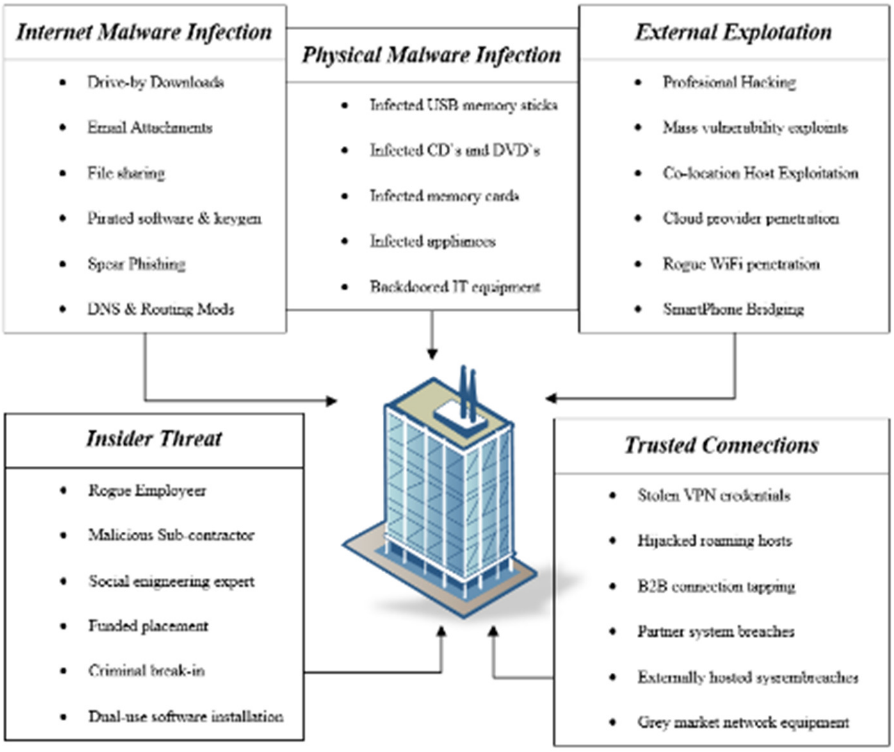

Figure 2. Breaching the enterprise

5. Approaches to adaptive forecasting of the directions of development of computer attacks in information systems

In the process of developing methods and approaches to organizing information and analytical support in complex analytical systems, including systems for detecting, preventing and eliminating the consequences of computer attacks, information security specialists are faced with the need to implement decision-making algorithms in conditions of vagueness and uncertainty of the source information.

Due to the fact that today the system for detecting, preventing and eliminating the consequences of computer attacks is not yet able to carry out its activities in a fully automated mode, a system of expert support is needed for its effective functioning.

In turn, the expert support system in the process of preparing solutions to respond to computer attacks and computer incidents caused by them relies on the results of the forecasting subsystem.

The structural and functional scheme of the forecasting subsystem can be represented in the form shown in Figure 3.

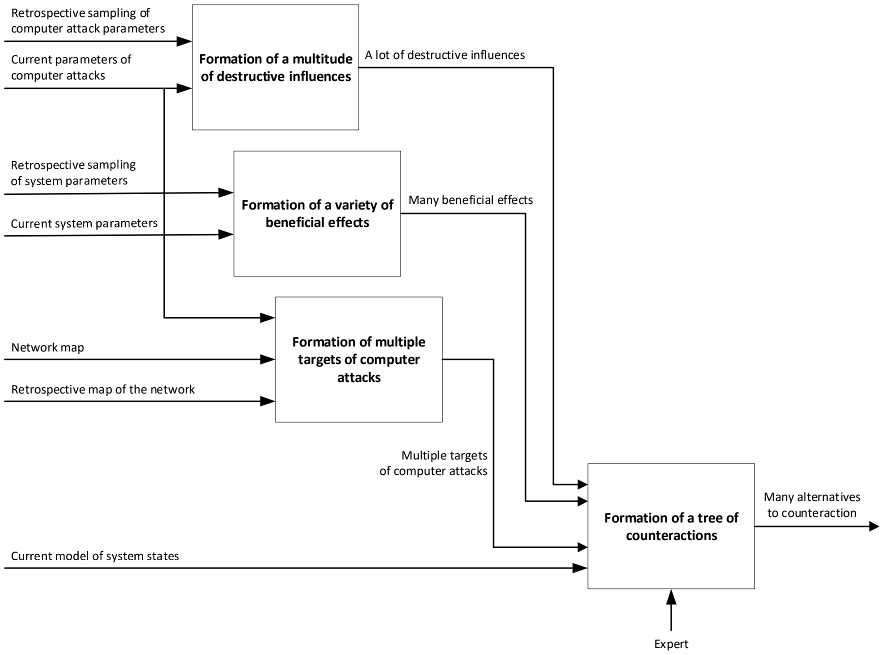
Retrospective sampling of computer attack parameters
Current parameters of computer attacks
Formation of a multitude of destructive influences
A lot of destructive influences
Retrospective sampling of system parameters
Current system parameters
Formation of a variety of beneficial effects
Many beneficial effects
Network map
Retrospective map of the network
Formation of multiple targets of computer attacks
Multiple targets of computer attacks
Current model of system states
Formation of a tree of counteractions
Many alternatives to counteraction
Expert

Figure 3. Structural and functional scheme of the forecasting subsystem

To determine the probabilistic values of the transition of an information system from one state to another, a mathematical model is constructed as a kind of aggregated object. As elements of the model, it is advisable to consider elements completed from the point of view of informational, functional and structural execution.

Based on such a construction and for the convenience of recording, the information system can be represented as a set of vulnerable elements to be protected:

$$\{e_m\} = \{e_1, e_2, \dots, e_m\}$$

Suppose that a set of threats, the implementation of which can be a destructive effect on the elements of the information system, of course, has N components:

$$\{y_n\} = \{y_1, y_2, \dots, y_n\}$$

Then, when building a model, it is necessary to consider the very possibility of implementing each threat from the set $\{y_n\}$ for each element of the information system from the set $\{e_m\}$.

The flow of threat implementation is:

- ordinary - threats appear one by one, i.e. the probability of two or more events hitting the area Δt is negligible compared to the probability of exactly one event hitting it;
- a stream without consequences – for any non-overlapping time segments, $\tau_1, \tau_2, \dots, \tau_n$ numbers equal to the number of events falling on these sections are independent random variables, i.e. the probability of any number of events falling on one of the sections does not depend on how many of them fell on the others.

Based on the limit theorem for the total flow, it can be concluded that the sum of the flows of various events on any element will converge to the Poisson flow, for which the statement is true:

- when adding any number *N* of independent ordinary flows, an ordinary flow will be obtained again, the intensity of which is equal to the sum of the intensities of the added flows. That is, for an element of the information system e_m, the intensity of the total flow of all threats from the set $\{y_n\}$ will be equal to:

$$\mu_m = \sum_{n=1}^{N} \mu_{nm}, \tag{1}$$

and for the intensity of the flow as a whole, it will be fair:

$$\mu = \sum_{m=1}^{M} \mu_m = \sum_{n=1}^{N} \sum_{m=1}^{M} \mu_{nm}. \tag{2}$$

where μ_{nm} is the intensity of the flow of the n threat to the m element of the information system.

According to (2), if the parameter μ of the Poisson law depends on time, that is, the flow of attacks is heterogeneous, then the probability of occurrence of α events in the time interval Δt is described by the expressions:

- for the element m and threat n:

$$P_{nm}[X(t, t+\Delta t) = \alpha] = \frac{1}{\alpha!}\left(\int_{t}^{t+\Delta t} \mu_{nm}(t)dt\right)^{\alpha} \exp\left(-\int_{t}^{t+\Delta t} \mu_{nm}(t)dt\right), \tag{3}$$

- for element m and set of threats Y:

$$P_m[X(t,t+\Delta t)=\alpha]=\frac{1}{\alpha!}\left(\int\limits_{t}^{t+\Delta t}\mu_m(t)dt\right)^{\alpha}\exp\left(-\int\limits_{t}^{t+\Delta t}\mu_m(t)dt\right), \qquad (4)$$

- for a protected system and a variety of threats Y:

$$P[X(t,t+\Delta t)=\alpha]=\frac{1}{\alpha!}\left(\int\limits_{t}^{t+\Delta t}\mu(t)dt\right)^{\alpha}\exp\left(-\int\limits_{t}^{t+\Delta t}\mu(t)dt\right). \qquad (5)$$

Thus, to build a model of the transition of a system from one state to another, it is necessary:

1) Identify many vulnerable elements of the system $\{e_m\}$.
2) Identify multiple potential threats $\{y_n\}$.
3) Associate with each element of the system e_m a subset of threats $\{y'_n\} \in \{y_n\}$, that can affect this element.
4) Make a table of intensities.
5) To determine the probabilistic characteristics of the flow of destructive effects on the element e_m.
6) To determine the probabilistic characteristics of the flow of destructive impacts on the information system.

The current parameters of the information system, a retrospective sample and a set of destructive influences are fed to the input of the module for the formation of a set of useful influences.

Functionally, the module consists of the following blocks:

- system parameters analysis unit;
- the block of analysis of a retrospective sample;
- a block for generating beneficial effects to counteract destructive ones.

In the process of analyzing the system parameters, many useful influences are formed (structured in the form of a tree) that can change the values of the controlled parameters, which will allow the system to switch to another state. A retrospective sample is needed in order to analyze the accumulated experience in countering destructive influences and choose the optimal beneficial effects.

To form a set of beneficial effects, it is necessary:

1) Determine the set of states of the information system into which a transition from the current one is possible.
2) To compare with each transition the probabilistic characteristics of the flow of realization of destructive influences.
3) To compare the beneficial effects determined during the formation of the model of the states of the information system.

The output data of the module is a set of useful effects on the system, structured in the form of a tree. This data is transmitted to the module for generating a variety of useful effects.

The current and retrospective network map, as well as the parameters of the current attack, are submitted to the input to the module for the formation of a set of computer attack targets.

The main task of the module is to predict the list of information system nodes and services functioning on them, which will be involved in the next stages of the life cycle of the current attack. [7] [8]

6. Conclusions

In studying the needs of information protection in our time to solve the problem was used to analyze the problem of technical vulnerability and incompetence of employees, the complexity of cyber threats, adaptive information protection, review of its benefits.

The structural picture shows the main tools of cyber threats and vectors of their penetration.

Also the requirements to the information protection system developed on the basis of principles of construction of adaptive system are formed, streams of realization of threats are considered, the mathematical model of transition of information system from one state to another is constructed and the structural scheme of subsystem of forecasting of computer attacks is offered.

REFERENCES

1. OZKAN B. Y., SPRUIT M., WONDOLLECK R., COLL V. B.: Modelling adaptive information security for SMEs in a cluster, Journal of Intellectual Capital, vol. 21, no. 2, pp. 235-256, 31 December 2019.
2. Casmir R.: A dynamic and adaptive information security awareness (DAISA) approach, Stockholm University/Royal Institute of Technology, no. 05-020, December 2005.
3. KIVIRISTI A.: Adaptive network security, ComputerPress, 1999.
4. BROOK A.: What is Adaptive Security? A Definition of Adaptive Security, Benefits, Best Practices, and More, Digital Guardian All rights reserved, 5 December 2018. [Online]. Available: *https://digitalguardian.com/blog/what-adaptive-security-definition-adaptive-security-benefits-best-practices-and-more*.
5. OZHIGANOVA M. I., KALITA A. O., TISHCHENKO Y. N.: Building adaptive information security systems, NBI technologies, vol. 13, no. 4, pp. 12-21, 2019.
6. RABAH K.: Industry 4.0 and Cybersecurity: Where is the Universities?, Mara International Journal of Scientific & Research Publications, vol. 2, no. 1, 15-33, 1 August 2018.
7. GOLITSYN S. A., SHULZHENKO A. D.: Approaches to adaptive forecasting of the directions of development of computer attacks in information systems, Science Magazine "GLOBUS”: Technical science, vol. 7, no. 1(37), pp. 44-49, 2021.
8. BASAN E. S., BASAN A. S., MAKAREVICH O. B., BABENKO L. K.: Studying the impact of active network attacks, Questions cybersecurity, no. 1(29), 35-44, 2019.