IEEE First International Conference on Data Stream Mining & Processing
23-27 August 2016, Lviv, Ukraine

Information Protection of Data Processing Center Against Cyber Attacks

Ogbu James Onyigwang, Yanina Shestak, Alexandr Oksiuk
Taras Shevchenko National University of Kyiv, Lomonosova Str., 81, Kyiv, Ukraine,
jamesybone@yahoo.com, lucenko.y@ukr.net, oksiuk@ukr.net

Abstract— **In this article, the most essential aims on information protection of data processing centers in more flexible way to provide the necessary level of security of the existing environment of development and dissemination of cyber-attacks, which should be easily scaled to support any of its changes in the future, also in this paper Formation of competitive information security of data processing center are analyzed Special attention is paid to avoidance of unauthorized access to information, its blocking, giving, destruction, dissemination, modification, copying, as well as ensuring functioning of data processing centers in a normal mode, in compliance with limit values of design parameters, execution of the target functions of data processing centers.**

Keywords— data, data security, data threats, cyber-attack, cyber security, cyber threat, strategy, and data protection

I. Introduction

In the conditions of steady development of the complexity and power of cyber-attacks aimed at corporate customers, there is a need to increase the demand for services of data processing centers (DPC) for the protection of servers, applications and resources against a wide range of attacks, including DDoS, attacks on vulnerabilities and web applications. One of the main issues of quality DPC protection is a comprehensive approach and application of systems to detect cyber-attacks, which include network and system sensors, security analysis system agents, mock systems.

Network and system sensors are the agents to detect system-level computer attacks and contribute to timely and critical monitoring of the major and critical network resources being protected. The basic rule when placing network and system sensors is that they should disperse in segments or on nodes with valuable information resources to achieve the highest level of protection [2].

The agents of detecting system-level attacks operate at the level of a network and at the level of a node. The latter are placed on the database servers, Web-servers and on all major network nodes. The network sensors are more common and are installed between the router and firewall to monitor all traffic that enters the network, and all outgoing traffic that is not blocked by a firewall. This placement helps protect the firewall. The next is to place in a “demilitarized zone” to protect Web-, FTP- and SMTP-servers as well as external DNS-server [3].

This is followed by placing between the firewall that allows tracking changes in the firewall’s operation and review all communications that pass through the firewall. Network sensor, in this case, is a means for monitoring the effectiveness of the firewall configuration.

The network sensors integrated into the switch became widespread today. This solution provides high performance and lack of switch capacity reduction, and the ability to analyze traffic of several VLAN.

The agents of detecting system-level attacks collect information that reflects the activity that takes place in a separate operating system in order to timely detect intrusion of the attack.

The main advantages of the use of system-level sensors of the modern DPC are the following: access control to information in the form of analysis of incoming and outgoing connections; displaying abnormal activity of a particular user; tracking change in operating modes associated with abuse; work in a secure network environment and the switch network environment.

However, despite a number of benefits, the agents of detecting computer attacks and have several shortcomings: network activity is not visible for system-level sensors; the use of auditing mechanisms, in most cases, requires the use of additional resources; while generating report on the information regarding incoming and outgoing connections you need a fairly large volume of disk storage space; OS vulnerabilities could affect the integrity of the system-level sensors; the cost of implementation and operation of agents of detecting system-level attacks is several times higher than in other approaches.

II. General concepts of information security in DPC

Within the framework of practical application, regardless of ownership of data processing center, the management staff faces a difficult task of ensuring security and integrity of the information to be stored in DPC. Special attention is paid to avoidance of unauthorized access to information, its blocking, giving, destruction, dissemination, modification, copying, as well as ensuring functioning of data processing centers in a normal mode, in compliance with limit values of design

978-1-5090-3736-0/16/$31.00 ©2016 IEEE

parameters, execution of the target functions of data processing centers [1].

Model of ensuring information security of DPC is shown in “Fig. 1”.

The main target area of protection DPCs against cyber attacks is complete minimizing of the possible damage caused by internal and external influences, as well as their prediction and prevention.

Building an information security system for DPCs is based on common principles. This is, above all, modeling of network access “Fig. 2” and building a threat model “Fig. 3”, Network access modelling based on the mechanism of restructuring relative to three directions and the selection of the most vulnerable places regarding cyber attacks. To select objects, which threats may be, directed to, i.e. through the assessment of vulnerability, integrity, observability, confidentiality, privacy, the analysis of each object is carried out and the possibility of penetration of a particular threat is argued, the level of potential harm (damage) is analyzed in qualitative and quantitative terms. Formation of risk model for each single functional system. As a consequence, we get a model of risk events, the degree of feasibility, the level of their impact, the extent of impact on the system and possible loss of information.

Network access modeling is based on identifying direction of all possible access channels to detect possible violations of policies of DPC network access isolation.

The structure of information protection against cyber-attacks in DPC is based on maintaining the model of “Plan-Do-Check-Act, PDCA” which is used to create an effective security system in the modern DPC.

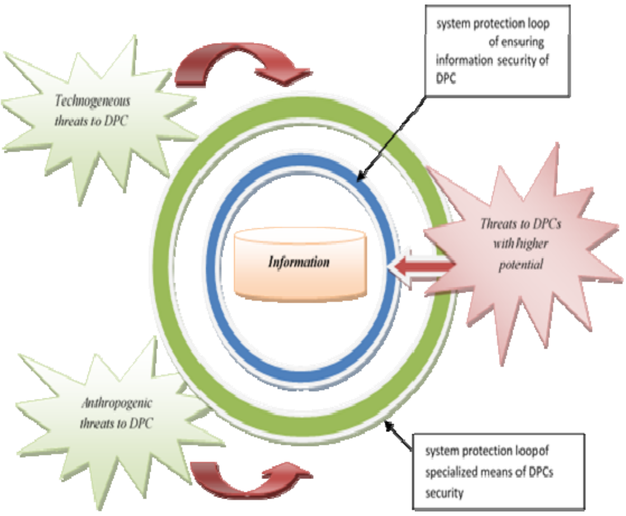
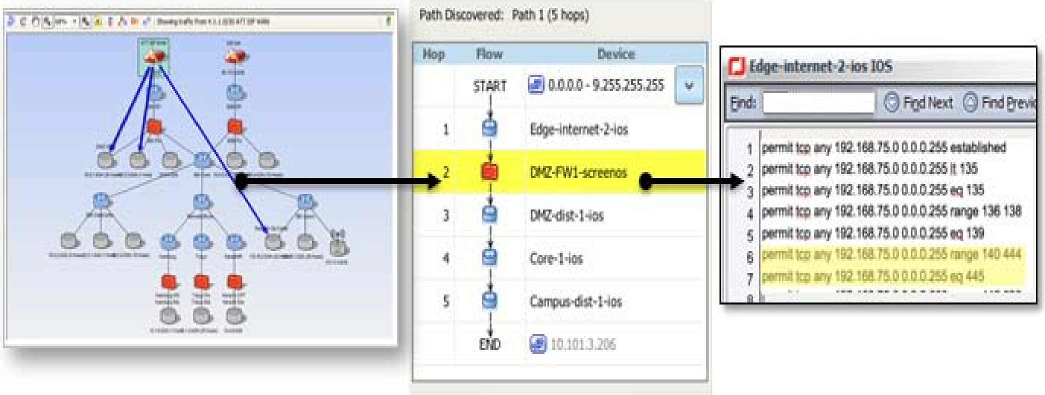

system protection loop of ensuring information security of DPC
Technogeneous threats to DPC
Information
Threats to DPCs with higher potential
Anthropogenic threats to DPC
system protection loopof specialized means of DPCs security

Figure 1. Model of ensuring DPCs information security.

Formation of competitive information security of data processing center in its fundamental basis consists of three main sectors.



Path Discovered: Path 1 (5 hops)

Hop	Flow	Device
	START	0.0.0.0 - 9.255.255.255
1		Edge-internet-2-ios
2		DMZ-FW1-screenos
3		DMZ-dist-1-ios
4		Core-1-ios
5		Campus-dist-1-ios
	END	10.101.3.206

Edge-internet-2-ios IOS

Find: Find Next Find Previ

```
permit tcp any 192.168.75.0 0.0.0.255 established
permit tcp any 192.168.75.0 0.0.0.255 lt 135
permit tcp any 192.168.75.0 0.0.0.255 eq 135
permit tcp any 192.168.75.0 0.0.0.255 range 136 138
permit tcp any 192.168.75.0 0.0.0.255 eq 139
permit tcp any 192.168.75.0 0.0.0.255 range 140 444
permit tcp any 192.168.75.0 0.0.0.255 eq 445
```

Figure 2. Network access modeling

Security threat model maps at the network chart possible vectors of attacks, both direct and indirect. To implement them compromising intermediate nodes of the network is required.

The first sector is a sector of network security. This sector in its structure contains the aggregation switch which operates at the level of the 2nd or 3rd OSI model and can aggregate data from multiple physical ports; root routers represented by service software that ensures data and instruction exchange between the objects in the system; load balancer that ensures distribution of tasks between multiple network devices; firewall which controls filtering of network packets passing through it in accordance with set rules; device that ensures encryption of traffic (especially when connected to the Internet) directed from the internal network to external network based on SKIP protocol, as well as filtering and decryption of traffic coming from the external network to the internal one; intrusion detection (IDS) and prevention (IPS) systems that monitor the network, users and identify facts of abnormal or dangerous network activity; antivirus.

The second sector is the server security sector. This sector implies switches designed to connect multiple units of a computer network within one or more network segments, where VLAN technology for isolation of access and information flow is the priority direction; servers designed to perform the service software support under the given conditions. Proceeding from the assumption, in most cases, it is the server part that is responsible for the communication with the network control center, where Security Operation Center (SOC) can be located. Access Control System and Identification The third is data storage sector. The structure of this sector is made up by disk arrays representing an external storage device consisting of multiple hard drives for storing massive information arrays; backup servers that ensure implementation of service software aimed at the backup of the information in order to increase the level of security; tape libraries which action is based on the recording and playback of information, its archiving and data backing up.

Detection Management (IDM) are installed in the same place [2].

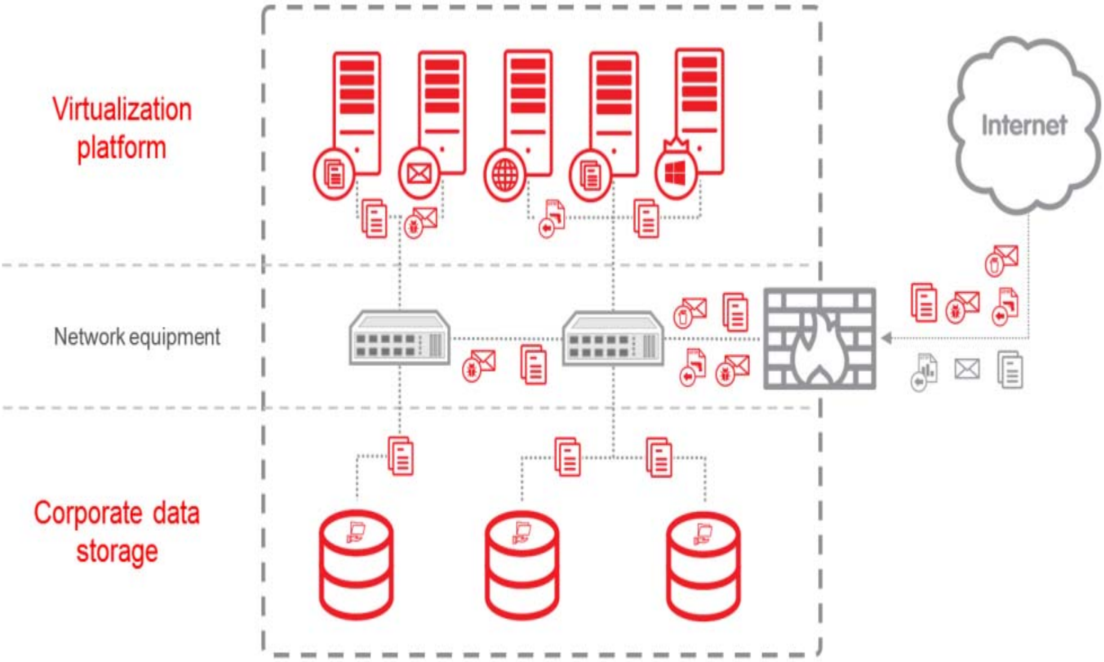


Figure 3. Security threats model.

Data storage sector is the main one and therefore calls for the introduction of advanced mechanisms to ensure data integrity. The priority direction in this area is Dense Wavelength Division Multiplexing (DWDM) technology. The essence of this technology is in the possibility of organizing a plurality of separate signals SDH by a single fiber, and, consequently, multiple increase of throughput [3].

In the current conditions, the issues in operation of data processing centers (DPC) become particularly urgent, which can significantly reduce the availability and the quality of DPC services. These issues are crucial to the success of customers and owners of DPC [5].

Monitoring of the network of data processing center is a systematic control over basic parameters of operation of the network and network applications to provide high levels of quality of user service and network performance. The systems of network monitoring accelerate the detection and analysis of the network problems encountered, and allow identifying potential problems and fix them before they impact the work of the customers of data processing center. The operators of data processing centers should invest in net flow monitoring tools to enable analysis of incidents and threats. Using a variety of tools — from Net Flow analysis to correlation of events using SIEM systems —the operators need to understand and assess the source

and types of internal and external threats. Comprehensive monitoring of processes and net flow helps identify unauthorized access to data, and timely identify threats of its accessibility before the customer notifies of the problem.

Today, as part of the international community, some areas (methodologies) of the network monitoring are singled out. One of them is SNMP monitoring (SNMP — Simple Network Management Protocol) —this is a widely used technology, which is generally intended to manage networking equipment (routers, switches, servers, etc.) SNMP monitoring provides details on the networking equipment and creates an overall picture of the network usage. However, despite the functions performed, this technology with a large number of controlled devices of SNMP inquiry may create a great net flow, that is an additional load on the controlled network. It is also worth noting that Simple Network Management Protocol which information is generally not sufficient to determine the root cause of the networking problems provides SNMP monitoring.

The second area of network monitoring is flow-based monitoring. Flow-based monitoring is an advantageous area due to its low-cost solutions, because routers and switches are usually used as sensors, eliminating the need to purchase additional devices for capturing traffic. As a result of this area of monitoring, the user receives useful statistical information about the network operation, applications and network bandwidth used. However, such monitoring methodology, depending on the type of technology used (xFlow) and the load on the networking equipment, can exercise sampled control of batches, reducing accuracy of generated information on the network.

Batch-based monitoring is also a relevant monitoring methodology of the network of data processing center. Batch-based monitoring systems analyze all parts of each IP batch (including its payload). These systems are able to generate the same statistics generated by SNMP- and flow-based solutions, thereby providing the most detailed analysis of the network operation [1]. The use of batch-based systems is the only way to quickly and effectively solves networking problems with no impact on the operation of controlled network.

The usefulness of the data processing center network monitoring is to accelerate the response to failures in the network and diagnose problems in the applications that are interspersed; investigation of network incidents and monitoring of compliance with the rules of using the customer's applications; optimization of network operation and acceleration of return on such IT initiatives as VDI and SDN; notification of traffic spikes and bandwidth planning. A data center (sometimes spelled datacenter) is a centralized repository, either physical or virtual, for the storage, management, and dissemination of data and information organized around a particular body of knowledge or pertaining to a particular business. A data center is a facility used to house computer systems and associated components, such as telecommunication and storage systems it generally includes redundant or backup power supply redundant data communications connections, environmental controls and various security devices. Large data centers are industrial scale operations using as much electricity as a small town.

Introduced the novel concept of stochastic cyber-attack process, which offers a new perspective for studying cyber-attack sand, in particular, can be instantiated at multiple resolutions such as network-level, victim-level and port-level [4]. Then proposed a statistical framework that is centered on identifying. In this paper, we identified the most critical security goals in the distribution automation system and proposed efficient ways of achieving these goals.

The message authentication and integrity is far more important than any other security requirements in the distribution system applications. The proposed protocols impose a negligible computation burden on FRTU, resulting in less time overhead on the DAS operation than the one when the encryption algorithms are used. Vulnerability assessment is a critical task to ensure that power infrastructure cyber security is systematically evaluated. The proposed analytical framework provides a measure to quantify the system vulnerability

Solutions aimed at the information protection of data processing centers must be flexible: providing the necessary level of security of the existing environment of development and dissemination of cyber-attacks, they should be easily scaled to support any of its changes in the future. The implementation, application and development of specialized technologies for protection of data storage systems and virtual environments is also an important aspect.

III. Conclusions

A data center (sometimes-spelled datacenter) is a centralized repository, either physical or virtual, for the storage, management, and dissemination of data and information organized around a particular body of knowledge or pertaining to a particular business. A data center is a facility used to house computer systems and associated components, such as telecommunications and storage systems. It generally includes redundant or backup power supplies, redundant data communications connections, environmental controls and various security devices. Large data centers are industrial scale operations using as much electricity as a small town.

Introduced the novel concept of stochastic cyber-attack process, which offers a new perspective for studying cyber-attack sand, in particular, can be instantiated at multiple resolutions such as network-level, victim-level and port-level. Then proposed a statistical framework that is centered on identifying. In this paper, we identified the most critical security goals in the distribution automation system and proposed efficient ways of achieving these goals.

References

[1] A. Zasetsky and V. Shelgov, "Monitoring of the Network of DPC", *Network Solutions Journa*l, LAN, vol. 05, 2013, pp. 68.

[2] A. Barskov, "The World of DPC-2015: Under the Sign "M"", *Network Solutions Journal, LAN*, vol. 05-06, 2015, pp. 76.

[3] A. Koshelev and A. Filchakov, "Fibre Optic Networks and DWDM Technology", *ComputerPress Journal,* vol. 1, 2001, pp. 45-48.

[4] J. Matusitz, "The Role of Intercultural Communication in Cyberterrorism", *Journal of Human Behavior in the Social Environment*, vol. 24, 2014, pp. 775-790.

[5] A. Barskov, The World of DPC -2015: Under the "M" Sign, The Journal of Networking Solutions, LAN, vol. 05-06, 2015, pp. 76.