Intelligent Information Management and Ensure Their Confidentiality

Varisov Akmal Abbasovich, Kerimov Kamil Fikratovich
Corresponding Author email: sa-said@mail.ru

Abstract: In article questions of the protection of information with using intelligent management of information resources of the government, e-government, and other sources of information. Apart from this eliminates the problem of data confidentiality.

Keywords: Safety Information, Management, Confidentiality, Information Security, Private, Traditional, Data, Significant Intellectual Data

1. INTRODUCTION

To meet the needs of the population in a more qualitative and broader access to public service government agencies around the world are evolving into e-government. In an ever ongoing changes in government organizations need a flexible framework within which they could build their IT-systems and software tools for the development and expansion of the services provided, not only on the internet.

Every year on the market "Safety information" are new telecommunications and IT systems, as well as methods to protect your data from intruders. But hackers are not far behind. Every year there are new types and the requirement for a security policy, security architecture and security systems, etc..

In today's world organization of personal data protection officials, including state, is one of the most pressing problems. The national interests of the Republic of Uzbekistan in the sphere of information are in compliance with the constitutional rights and freedoms of citizens in the field of information and its use in the development of modern telecommunication technologies in the protection of state information resources from unauthorized access.

The relevance and importance of the issue of security of personal data caused by such factors as:

- increase in computing power;
- increase of information collected, stored and processed by computers and other automation equipment;
- concentration in single database of information for different purposes and different accessories;
- expanding the range of users who have direct access to computing resources and data sets;
- rapid development of software tools that do not meet even the minimum safety requirements;
- ubiquitous networking technology, combining local networks to the global;
- development of the global Internet, virtually preventing security breaches of information processing systems worldwide.

Information security is usually considered as the sum of the following three basic properties of protected information:

- privacy, meaning that access to information can be obtained only legitimate users;
- integrity, which means that, firstly, the protected information can be changed only by legal and unauthorized user, and secondly, the internal consistency of the information, and (if the property is applicable) reflects the real state of things;
- availability, guaranteeing free access to protected information for legitimate users.

Key control measures in terms of legislation are:

- ensuring the confidentiality of personal data;
- protection credentials of the organization;
- intellectual property rights.

Practice shows that for the successful implementation of information security in an organization decides to include the following factors:

- that the objectives, policies and procedures for information security business objectives;
- coordinated approach to the implementation of security systems with the corporate culture;
- visible support and commitment from management;
- a clear understanding of the requirements of security, risk assessment and risk management;
- ensure understanding of the need for information security measures management and staff of the organization;
- transfer instructions in respect of information security policy and standards to all employees and contractors;
- providing the necessary education and training;
- comprehensive and balanced system of measurement indicators used to evaluate the effectiveness of information security management and proposals for improvement received from performers.

The functions of the proposed information security services of the state body that ensures the protection of personal data of employees:

- organization and coordination of activities related to the protection of information the public authority;
- study of information processing technology in order to identify possible leakage paths and other information security threats, the formation of a threat model, the development of security policy information, the definition of measures aimed at its implementation;
- the development of draft regulatory and administrative documents, operating within the state body, in accordance with which information must be provided to protect the public agency;
- identification and neutralization of threats;
- registration, collection, storage, processing of all events in the system that are relevant to information security;
Formation of staff and users understand the need for a public authority comply with legal acts, regulations and regulatory documents related to the protection of information.

Currently, there are a large number of organizational and technical measures that can be used to protect against phishing attacks. Organizational measures related to the development and implementation of enterprise legal documents defining the requirements for information security information systems (IS). Examples of such documents are policy and the concept of information security, job descriptions of staff to work with IP, etc. Technical same protection ICs implemented using appropriate software, hardware or software and hardware systems.

To date, the following main types of technical means of protection of personal data:
✓ means of cryptographic protection of information;
✓ means of access to the resources of the users of IP;
✓ means of firewall;
✓ analysis tools security of information systems;
✓ intrusion detection;
✓ anti-virus protection;
✓ means of content analysis;
✓ anti-spam.

Safe and reliable processing and transmission of information on the domestic market in the external current conditions of economic globalization are extremely urgent task for the state, the solution of which serves to strengthen its economic security.

Among the new threats to security should be a new approach to security management. The Security Division of required safety analysis architecture that can handle much more volume and a wider range of data than is currently not to mention the media, allowing to quickly solve the most serious problems. They need intelligent data about threats, including the latest tools, techniques and procedures used by attackers as well as the ability to manage response procedures that are performed after the detection of problems.

According to a report by Verizon «2012 Data Breach Investigations Report» 99 percent resulted in vulnerability to the data being compromised during the few days or less, while 85 percent to investigate vulnerabilities took several weeks. This is a serious challenge for security departments, as attackers get a lot of time to work in a compromised environment. More “free time” leads to more stolen data and more serious damage.

This is mainly due to the fact that the current security measures are not intended to deal with more complex threats. Traditional security measures often have the following characteristics.
✓ based on signatures: Searches "known malicious" data sequences based on previous identical attacks;
✓ Oriented to the perimeter: focus on the prevention or detection of threats to the organization;
✓ based on the requirements of regulators: designed to meet the requirements of auditors or specific legislative instruments to a greater extent than to eliminate the most serious risks to the organization.

At the same time, threats are becoming more complex. Modern threats have the following characteristics.
✓ Efficiency: they anticipate the means used by organizations to protect themselves, and use adaptive techniques to circumvent many of the common systems, intrusion detection and prevention;
✓ Concentration: today's threats are often set themselves certain tasks, and can be targeted to a narrow class of organizations or even a single organization;
✓ Intelligence: they use a wide range of techniques of social engineering and technical support for the creation of vulnerability in targeted organizations and to prevent detection.

This means that the organization should start a different attitude to the means and methods of their protection.

Many companies believe that traditional systems SIEM benefited by providing the following features.
✓ Create reports OS active devices such analytical information about current critical actions: who, what, where and when;
✓ Basic Alert on known sequences using correlation rules that can draw attention to the most suspicious transactions to the computing resources;
✓ Certificate regulatory compliance for internal and external auditors in the form of regular reports created automatically, rather than manually generated for each audit or evaluation of each;
✓ Centralized view different event sources collected, allowing security units will make decisions based on information obtained from a variety of sources.

However, in modern conditions it is necessary to take into account the new requirements. The latest attacks are carried out not only by vandals or lovers, but also experienced criminal groups and even states. These criminals use sophisticated techniques, such as delete their traces in the log files and reduce to a minimum the number
of verifiable events. Therefore, traditional SIEM systems are not enough. Organizations should adopt a more innovative approach to protect against this threat.

In the world of contemporary threats to security teams need to quickly determine how the attack took place, in order to reduce the time available since the invasion attacker Wednesday until an infrastructure, and apply measures to prevent such attacks in the future. With this in mind, the company believes that organizations need a more efficient platform that solves the problems of a growing number of security management for the following reasons:

-**complex threats require visibility of network traffic and event data across the enterprise:** the actual network traffic or event data do not provide enough information for the detection and investigation of these types of threats;
- **Security is now a big problem for data analysts SOC:** SOC analysts now need to learn much more dynamic and heterogeneous set of data to detect complex threats, which requires a combination of internal and external analysts;
- **The compromise is inevitable:** a realistic goal - not to resist all attacks and to respond quickly to prevent damage and minimize the impact on the business.

2. **CONCLUSION**

Find the most complex threats can be very difficult. Often, the most obvious signs of threats on the network appear exactly as they enter the IT infrastructure and distributed secretly withdrawn from it. Therefore, a record of all network packets in the following order.

Determine getting malware on Wednesday and prioritize related activities. Modern malware is very similar to any other application that scans the network, but the full package enables organizations to isolate and restore executable files, and automate much of the analysis required to identify evidence of the work of the attacker. This in turn can help analysts identify malicious programs with the highest priority issues to be addressed first.

Track side movement attacker after penetration. When the attackers create their own foothold in the organization's IT environment, they often move from one end point to another, collecting the necessary information for the next phase of the attack. Since these endpoints are rarely monitored centrally, requires full network packet for information about this move in the organization.

Confirm exactly what happened and what data has been transferred. Many complex threats will not be detected prior to the attack, and even after its completion. At this point, security units need to assess the damage, recreating the attack and determine what data is stolen and whether it is encrypted.

In the new information age where most sectors of the state is controlled by intelligent machines, the question arises, why not use an intelligent system for the protection of information? Intelligent Protection System solves many acute problems as human factors in data protection and decide faster than we are, and especially factors lead to these decisions. In many states, these types of systems are already used in different sectors of government. For example: in Belarus intelligent control system of commodity-traffic based on automatic identification technologies and electronic document management (RFID-technology).

RFID-technologies provide higher processing performance information, completely eliminating the need for human contact with them during processing. If you use such technology in the "electronic government" of the effect it would have been enormous.

Such technology is one of the specific examples of the phased implementation of a single information space. As part of its work provides the formation of a unified system of accounting information according to established rules, allowing the sharing of various automatic identification systems of two-dimensional codes. The transition from paper to electronic. Work on establishing a common information resources containing electronic passports for their uniform use in various information systems - production, logistics, and others.

New approaches to security management based on four main elements.

![Fig. 2.](image-url)

Approach to security management based on big data. Distributed data architecture allows customers to collect and analyze data security with unprecedented scale and speed changes.

- This approach seeks to make available a set of tools for the analysis of safety data, support the basic operations analysts - from the notification and reporting to analyze malware.
- The level of control that binds the security analyst to business. The unique product portfolio helps customers simplify the process of collecting information about the company's critical business processes and systems, as well as business requirements for their protection.

Copyright © 2015 IJEIR, All right reserved

238
Analysis of the threats, allowing customers to receive timely information. Distribution of current analytical data about the threats for products, enabling organizations to connect with their analytics environments.

Significant intellectual data. Threat analysis performed. Helps security analysts to get the maximum benefit from the feeds with the latest information about threats.

Full management of information molasses enterprise and security of information resources using high-speed computers gives a great advantage in the field of control and data storage and protection.

REFERENCES

[3] Strategic Intelligence: Business Intelligence, Competitive Intelligence, and Knowledge Management

AUTHOR’S PROFILE

A. A. Varisov, assistant in Department of Systems and application programming. Assistant Professor, and research associate in the Department of Information Security at Tashkent university of information technologies In Uzbekistan. He has published more than 10 papers in international journals and conference proceeding.

A.A. Varisov is assistant professor of Computer Science. He has been a practicing Educational Consultant for Information Security, E-Government, evolution funded projects of ERASMUS MUNDUS, With Security organizations, with university’s and many companies. His current research interests include orchestrating framework in cloud computing, data mining.

Ph.D K.F. Kerimov, Head Department of Systems and application programming Professor and research associate in the many Departments of university Information technologies. He has published more than 19 papers in international journals and conference proceeding.

Ph.D K.F. Kerimov professor of Computer Science. He has been a practicing Educational Consultant for Information Programming evolution funded projects of with a lot organizations, companies. His current research interests include orchestrating framework in cloud computing, data mining.