Volume XXIII 2020
ISSUE no.2
MBNA Publishing House Constanta 2020

Scientific Bulletin of Naval Academy

SBNA PAPER • OPEN ACCESS

Innovative system for detecting information attacks. The theoretical basis of the future research

To cite this article: Violeta Nicoleta Opriș, Scientific Bulletin of Naval Academy, Vol. XXIII 2020, pg.172-176.

Available online at www.anmb.ro

ISSN: 2392-8956; ISSN-L: 1454-864X

doi: 10.21279/1454-864X-20-I2-023

Innovative system for detecting information attacks. The theoretical basis of the future research.

Violeta Nicoleta Opriș
Ph.D., Teaching Assistant
Titu Maiorescu University Bucharest
violeta.opris@gmail.com, violeta.opris@prof.utm.ro

Abstract: Computer security and maintaining the high level of security is an obvious problem in the virtualized society. The implementation of the innovative management system requires detailed planning and offers precise detection actions. There are different classifications of innovative information systems, depending on interpretation, control and anticipation: diagnosis, repair, training, interpretation, prognosis, design, planning, monitoring, control, maintenance, prediction, simulation, classification and taxonomy.

1. Introduction

The central idea of the paper is based on research on the implementation of an innovative management system to maintain an increased level of security in virtual environments and on annual Gartner Reports 2018, regarding the types and the large number of vulnerabilities of Cloud computing [9]. According to the Gartner study, named Cloud Computing Top List of Emerging Risks, September 2018, Cloud computing is growing in popularity and becoming a solution to the problems that have plagued IT organizations over the years. Estimated, by 2020 the number of cloud service providers will triple. While organizations are trying to expand cloud services as an integral part of digital business initiatives, there are concerns about information risks.

The innovative system designed by the management in this paper can be integrated with future intrusion prevention systems. It includes components for analyzing, deleting, detected intrusions and event planning. At the same time, there will exist the possibility of integration with the systems in operation and the construction of an integration pilot with the external systems. Also, a knowledge base, a user interface, a planned scan module, another ticket assignment module will be designed to solve specific problems and the addition of new connections. The computer system uses an algorithm for precise planning.

Analyzing the database of the Institute of Standardization and Technology (NIST - NVD National Vulnerability Database) it is noted that SQL injections and XSS attacks are the most widespread ways to alter the information in the databases. NVD is the US Government's repository for vulnerability management standards [10]. These data allow for the automation of vulnerability management, security measures and compliance. NVD includes databases with reference to security checklists, security flaws, misconceptions, product names and impact. These are presented in table 1.1 according to the vulnerability id, description and impact [10]:

ID vulnerability	Description	Impact
CVE-2017-3221	SQL injections into Inmarsat AmosConnect 8 login forms allow remote attackers to access user credentials, including usernames and passwords. Posted: July 22, 2017; 04:29:00 PM -04: 00	***V3:*** **9.8CRITIC** ***V2:*** **5.0MEDIUM**

CVE-2016-2351	Vulnerabilities with SQL injections in home / seos / courier / security_key2.api on FTA before FTA 9 12 40 allows remote attackers to execute SQL commands by injecting the client_id parameter. Posted: May 07, 2016; 10:59:04 AM -04: 00	***V3:*** **9.8CRITIC** ***V2:*** **7.5HIGH**
CVE-2016-5048	Vulnerability with SQL injections in chat / staff / default.aspx in ReadyDesk 9.1 allows remote attackers to execute SQL commands through the User Name field. Posted: August 26, 2016; 03:59:09 PM -04: 00	***V3:*** **9.8CRITIC** ***V2:*** **.5HIGH**
CVE-2016-5061	Multiple cross-site scripting (XSS) vulnerabilities on the Aternity web server before version 9.0.1 allow attackers to inject HTML script through (1) HTTPAgent, (2) MacAgent, (3) getExternalURL, or (4) retrieveTrustedUrl page. Posted: September 29, 2016; 06:59:00 AM -04: 00	***V3:*** **6.1MEDIU** ***V2:*** **4.3MEDIU**
CVE-2016-4969	Cross-site scripting (XSS) vulnerability in Fortinet FortiWan (formerly AscernLink) before version 4.2.5 1 allows attackers to inject HTML script via IP parameter into script / statistics / getconn.php. Posted: September 21, 2016; 10:25:11 AM -04: 00	***V3:*** **6.1MEDIU** ***V2:*** **4.3MEDIU**
CVE-2016-2350	Multiple cross-site scripting (XSS) vulnerabilities on FTA before FTA_9_12_40 1 allow attackers to inject web script or HTML through unspecified entries in (1) getimageajax.php, (2) move_partition_frame.html, or (3) wmInfo.html Posted: May 07, 2016; 10:59:03 AM -04: 00	***V3:*** **6.1MEDIU** ***V2:*** **4.3MEDIU**

Table 1.SQL and XSS vulnerabilities

2. Expert system overview

In this section we will deal with a field of applicability of artificial intelligence, following the part of personal contributions to present the result of implementation, an innovative management system for the detection of information attacks on databases. The paper addresses the issue of computer security by implementing an innovative system for virtualized innovative centers. This section presents the specialized literature for expert systems, being the foundation of designing the innovative management system.

Developing the innovative system for increasing security is a complex path. It is represented by the threats and vulnerabilities of the virtualized society. The concepts for the development and implementation of innovative systems come from the branch that studies artificial intelligence (AI).

There are a myriad of definitions for an innovative system. They use names based on knowledge. Professors Robert J. Mockler and D.G. Dologite (1987) demonstrate that a knowledge-based system is capable of reproducing intelligent activities specific to human experts [4].

Professor at Stanford University, Edward Feigenbaum, parent of expert systems technology, defines the expert system (SE) as a smart program (1981). This type of system uses knowledge and inference procedures. It also aims to solve complex problems.

Another important definition, Professors J. Giarratano and Riley (NASA), define an expert system as a system that simulates the ability of the human expert to make decisions.

Louis E. Frenzel defines an expert system as a particular program. It incorporates a knowledge base and an inference engine, simulating an intelligent consultant in a specific field [5].

H. Farreny (1986) defines expert systems as programs intended to replace the expert in areas where the need for human expertise is recognized.

Also, Yang and Okrent stated in 1991 that expert systems are more convenient than human experts in a long-term process.

DENDRAL is the first expert system. This was noted when NASA (1960) sent a vehicle to Mars to investigate the chemical structure of the soil of this planet.

One of the oldest expert systems is MYCIN (1972), which influenced the history of expert systems development. It was developed at Stanford in the 1970s. It aimed to diagnose and recommend treatment for different blood infections. MYCIN has never been used in practice.

The concept of developing innovative systems is confined to the field of artificial intelligence. The first programming language was LISP in the US and Prolog in France.

The main components of the innovative management system designed are the knowledge base and the detection algorithm for anomalies in the databases. Thus, the system designed SysExp can be referred to as a program that monitors knowledge. It will aim to obtain results on complex detection activities.

The most important features of the innovative system are identified as the ability to process a complex amount of knowledge and detect problems at the database level. In the case of classical innovative systems, we distinguish different areas of interest on which research has been carried out during the evolution of information technologies: fuzzy systems and logic, neural networks, genetic algorithms, machine learning, data mining, intelligent agents, voice processing, hybrid intelligent systems, natural language processing and hybrid intelligent systems.

Innovative systems can be classified as follows: systems that think like people, that think rationally, that act like humans and that act rationally. Thus, the system designed in this paper will combine several features presented previously.

The designed system contains a detection algorithm, a knowledge base and a user interface. Also, this variant of architecture can be expanded by adding secondary components. Another important aspect is the large amount of knowledge gained from the scan, which needs to be managed in the system.

The innovative management system involve complex development stages. These are essential for meeting the initial functional requirements [1].

- Stage 1: Assessment of the problem;
- Stage 2: Knowledge analysis;
- Stage 3: Design and implementation;
- Stage 4: Testing;

- Stage 5: User Manual;
- Stage 6: Maintenance.

Stage 1 represents the appreciation of the problem, which involved identifying the problem and carrying out thorough research. The problem was identified from the analysis of the disadvantages offered by Cloud computing. These disadvantages carry risks regarding data protection.

Stage 2 is the knowledge analysis. It is a complex phase in the development of an innovative system and cyclical process. In this stage, the UML diagrams are made to obtain information that will be used later in the implementation stage.

Stage 3 represents the design and implementation. It consists of the selection of the knowledge representation technique and the control of the design strategy. Also, this stage involves designing the interfaces and implementing the fundamental algorithm for scanning and detecting intrusions from databases.

Stage 4 is testing. This stage is important because test scenarios are performed. Check if the innovative system achieves its the purpose without major deviations.

Stage 5 is the user manual. It consists of the technical documentation for the innovative system. Being a complex set of components, there is a need for documentation. At the same time, documentation is a necessary process for understanding all stages.

Stage 6 is a maintenance process. The innovative system will be continuously updated to meet the requirements requested by users, including the future requirements for extending the functionality of the system designed in this research paper. Currently, there are innovative systems used to solve problems in fields such as medicine, mathematics, engineering, computer science, defense and security. They can be interconnected with artificial neural network technologies, fuzzy logic, genetic algorithms and other methods of artificial intelligence.

3. Cloud computing technology

The concept of modernism of innovative systems involves the interconnection with cloud environments to solve certain problems regarding the security of information in the cloud.

Information systems migrate to an innovative research area. The interconnection of the infrastructure of innovative systems with Cloud computing is a complex process, which requires careful planning [3].

This complex process can have massive costs, interoperability and security breaches. They can also create significant obstacles when attacking. Cloud computing has essential benefits and most IT&C companies currently use it. In order to maintain security, security control mechanisms are also implemented.

The concept of developing an innovative detection management system is in the attention of the research community. Developing an innovative web-based system is a multidisciplinary and complex task. An important factor is the lack of general research and methodology. This is necessary for the development of innovative web-type systems.

Many studies on innovation start with the phrase "innovation is paramount to survival". When searching for this sentence in a search engine, thousands of results can be found. The process of technological innovation from the point of view of information systems begins with the technical discovery of new things or new ways of doing things. Nowadays, we are witnessing a considerable evolution of innovative systems based on artificial intelligence in all fields. Existing literature for innovative web-based systems is under development [2].

An important aspect of the development process is the fact that there are several factors. Factors can alter the development stages of an innovative system. By default, the limitation appears, influencing the complexity of innovative systems. Limitations may be process requirements, availability of cloud infrastructure, applied methodology for design, engineering expertise and complexity of end-user requirements.

Dokas and Alapetite (2006) presented a meta-model development process for web based expert systems with combined web and expert system engineering experience [6].

Frantti and Majanen (2014) explored an expert system of real-time traffic management in local wireless networks. Congestion is based on delay and flow control and real-time traffic downloads, from local wireless networks (WLANs) to mobile cellular networks (CMAs) on multi-

localized devices. The developed control system is based on an integrated hierarchical expert system [7].

Experts have designed various applications in multiple fields, such as medical, military, education. Barreto and Azevedo (1993) use neural networks as associative memories to build an expert system to support medical diagnosis [8].

Expert systems have become an instrument in operations control. These have a major impact by using the knowledge base. They also produce signals for efficient control of operations and processes.

4. Conclusions

The information is vulnerable and the most common issues appear at the network level. When evaluating the security level for databases of cloud systems, the following issues are taken into consideration: confidentiality - information should be accessible only to authorized cloud users, integrity - information is not unauthorized and availability - information must be accessible to cloud users at any time.

Redefining the concept of computer security is an essential requirement in the virtualized space called Cloud computing. Cyber warfare is already a done fact. For this reason, information security requires preventive and offensive actions.

An innovative management system was analyzed and developed so that it detects anomalies in databases, with the possibility of integration with Cloud computing.

With the help of the analysis carried out in the paper, it was possible to see how the classical systems can be improved. This research describe how the innovative system can be developed.

References

[1] Opriș,V.N., Building and modelling a sustainable expert system, using UML language, The 4th International Conference Sea-Conf, Academia Navală Mircea cel Bătrân, Constanța, 2018

[2] Opriș,V.N., Opriș,M.E., Expert Systems Running Across Multiple Clouds. A sustainable perspective, The 2nd INTERNATIONAL CONFERENCE SEA-CONF, Academia Navală Mircea Cel Bătrân, Constanța, 2016

[3] Dumitru, L.A., Eftimie S., Mihăilescu, M.I., Niță, S.L., Opriș,V.N, Răcuciu C., A Novel Architecture for Authenticating Scalable Resources in Hybrid Cloud, The 11th International Conference on Communications, București, 2016

[4] Mockler, R.J., Dologite, D.G. , Knowledge-Based Systems for Strategic Corporate Planning, 1987

[5] Louis, E. F., Crash course in artificial intelligence and expert system, 1987

[6] Dokas, I. M., Alapetite, A., A view on the web engineering nature of web based expert systems. In ICSOFT 2006 – International conference on software and data technologies pp. 280–283

[7] Frantti, T., Majanen, M., An expert system for real-time traffic management in wireless local area networks, Expert Systems with Applications 41, 2014, 4996–5008, 2011 Elsevier

[8] Barreto, J. M., Azevedo, F. M., Connectionist expert systems as medical decision aid. Artificial Intelligence in Medicine, 1993, 5(6), 515–523

[9] https://www.gartner.com/en/products/special-reports

[10] https://www.nist.gov