Journal of Theoretical and Applied Information Technology
30th April 2021. Vol.99. No 8

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

IOT DEVICES INTEGRATION AND PROTECTION IN AVAILABLE INFRASTRUCTURE OF A UNIVERSITY COMPUTER NETWORK

[1]BLOZVA A., [2]KYDYRALINA L.M., [3]MATUS Y.V., [4]OSYPOVA T.Y.,
[5]SAUANOVA K., [6]BRZHANOV R.T., [7]SHALABAYEVA M.

[1,3,4] Department of Computer System and Networks, National University of Life and Environmental Sciences of Ukraine, Ukraine
[2]Non-profit joint stock company "ShakarimUniversity in Semey", Educational Department of Physical and Mathematical Sciences and Informatics, Semey, Kazakhstan,
[5]Almaty University of Power Engineering and Telecommunications named Gumarbek Daukeyev, Almaty, Kazakhstan
[6]Department of Construction Engineering of the Caspian State University of Technology and Engineering named after Sh. Yesenov, Aktau, Kazakhstan
[7]PhD student, Kazakh University ways of Communications, Almaty, Kazakhstan

E-mail: [1]valss725@gmail.com, [2]lazat_75@mail.ru, [3]umatus@nubip.edu.ua, [4]t_osipova@nubip.edu.ua, [5]brzhanov@mail.ru, [6]klartag@mail.ru, [7]m.shalabaeva@mail.ru

ABSTRACT

With every passing year computer network security requires new approaches to its structure. Taking into consideration the development of IoT devices and their active integration in such networks this makes another challenge to the cybersecurity network engineer. This article is an attempt to disclose practical approaches to the design and implementation of a computer network of an educational institution (using the example of a university network), which recently have increasingly begun to suffer from outside interference. The possibility of using a web application firewall in such networks and corresponding software for security and incident response at the L5-L7 OSI level is considered. The results have been summed up and further directions of research have been determined.

Keywords: *Cybersecurity, Computer Network, Iot Device, Security Systems Integration*

1. INTRODUCTION

The Internet allows you to collect and transmit data in real time from any device or system connected to it. IoT systems use data from these devices for automate decision making and forecasting, and help enterprises respond more quickly and efficiently to business changes and operational needs. At its core Iot is a method of instrumentation, sounding and control of connected physical devices by IT installation into them [1, 2].

IoT fosters change in a variety of areas, including improved equipment maintenance and asset management, related products with new understandings of consumer behavior, supply chain automation, and new forms of collaboration between people and machines.

IoT systems even begin to penetrate the work of educational institutions. Climate condition monitoring in classrooms, learning labs, specialized rooms, in which research is carried out [3, 4]. There is a need to integrate these devices into the computer network of an educational institution and to protect them, considering rapid growth of various attacks and possible vulnerabilities.

With the recent expansion of IoT the number of devices connected to the network increases dramatically. Connected devices go beyond information devices. They include a wide variety of items, including items related to life, such as vehicles and medical equipment, items with a potentially large impact on society, such as power plants and nuclear constructions. Considering that IoT is made of various devices connected to the network, when one device is infiltrated by malicious software, it can be a starting point for spreading the penetration to other devices, ultimately threatening critical infrastructure that should normally be

protected. Past actual security incidents have demonstrated that software vulnerabilities for communication devices connected to critical infrastructure, such as work personal computers (PCs) and surveillance cameras are aimed at unauthorized access from outside. These devices were used as entry points for critical infrastructure to function properly.

Experts in cyber security know that hackers are constantly developing new methods. New threats are constantly emerging that need to be identified and contained so that resources and communications are restored as soon as possible. To make a profit, many hackers do not hesitate to use such methods as extortion, fraud and identity fraud. The need to constantly defend against these attacks has led to the creation of several response models to typical cyber attacks. But research in this direction is still relevant.

This article explores the security challenges associated with IoT adoption and approaches to solving them.

2. LITERATURE REVIEW

With recent advances in information and communication technology (ICT), various services are now offered, linking the Internet to objects [5, 6]. IoT is currently used in various fields, especially in multimedia services. IoT has many advantages in multimedia service environments, such as the ability to provide convenient transmission and reception of data and the new service markets expansion. However, these benefits are accompanied by security threats that can arise from different heterogeneous cable and wireless communication paths [7–10]. So current generation needs multimedia security studies to take into account the threats that may arise at endpoints (smart devices, cloud services, networks, etc.) of various platform environments [11–14].

Earlier cyberattacks tended to have been indiscriminately without an established target. However, attacks against modern multimedia service environments turn into targeted attacks on specific targets. Despite the fact that human and material resources are being invested to protect against cyber attacks around the world, these attacks continue to increase, and as a result, the amount of damage they cause had also increased [15-20]. So, information security (IS) for multimedia service environments is seen as one of the key topics that are of interest to leaders and decision makers in the world's leading corporations [21-23]. However, the resources that can be dedicated to address the growing cyber threats are limited.

Cyber threats have recently become more sophisticated and complex [22–25]. With a mind to better understanding and quickly responding to cyber threats in multimedia service environments we need a framework to analyze the concept of threats in a structured way. The Cyber Defense Chain Model is used in different ways as the framework explains modern persistent threats (MPT). Using this model, one can easily understand the processes of complex, advanced resilient threats in a multimedia service environment, and quickly establish counter-strategies against threats at each stage.

As the term «kill chain», attacks can be successfully blocked by breaking a link at each stage of a chain-linked threat. However, IoT-based endpoints, including people, objects, and services, are easily penetrated by phishing, SMishing, and social engineering attacks, and an attacker can infiltrate an organization using these attacks.

Many years have gone since the introduction of the cyber kill chain model as a basis for understanding of advanced persistent threats in information security. Although our threat understanding has improved through this model, there are also endless accidents due to advanced persistent threats. There has been very little research into securing endpoints within an organization in a multimedia service environment. Moreover, researchers continue to argue that the kill chain models in the existing cyber security field are not enough to explain the threats arising in the organization. If the model explaining the threat is inaccurate or incomplete, counter-strategy formed against these threats will inevitably be inadequate [26-30].

Finally, we will analyze the characteristics and limitations of cyber security chain models (linear and circular models) that have been proposed in the information security field. On the basis of this analysis we propose a revised cybersecurity model that may explain threats within an organization, that have not been accurately expressed in existing models of the kill chain at higher educational establishments.

3. PURPOSE OF THE ARTICLE

The main purpose of the study is to review and analyze the methods and technologies for integrating and protecting IoT devices in a computer network by the example of a higher education institution network.

To achieve the goal we consider the use of a web application firewall and related software for security control and incident response at the L5–L7 OSI level in such networks of educational institutions. It is also

necessary to conduct preliminary network testing to assess the possibility of:

1) responding to L3–L4 attacks using standard firewall capabilities;

2) responding to interference at the upper levels of the OSI L5–L7 model, namely: SQL injection, distributed DDoS, botnet networks' attacks.

4. METHODS AND MODELS

During research the following methods were used: methods of system analysis and theory of complex systems with the application of mathematical models and methods of discrete mathematics – to describe the hierarchical information network of the university and transitions of the random process of functioning; theoretical foundations of functional stability and security of the university's information network, based on the principles of the reliability theory, the theory of optimal systems, functional modeling theory, methods of expert assessments, combinatorial theory and analytical modeling to improve the mathematical model of functional stability for software-defined networks; general statements of the queueing technique for improving the methods of choosing the optimal option of a cybersecurity system architecting of the university's network.

Computer network compositing of an educational establishment, for example, university, college etc (hereinafter referred to as university), as a rule, is standard. So, there is one connection to the Internet Service Provider (ISP) which selects some allowed IP addresses for network access providing. There is one router at the perimeter of the network, to which, in turn, the switching core is connected. Distribution level moves to each individual building / class. Different circumstances and sizes of the university should be taken into account, but construction and deployment principle is the same. Network server segment was selected in a separate VLAN. A chosen channel was turned to it. Such architecture scheme is quite simple and does not require large, both material and physical costs for its deployment and support.

Increasingly, IoT devices are beginning to be introduced into the infrastructure of an educational establishment. Certain devices monitor temperature, humidity and pressure and smoke contamination in classrooms. Certain devices serve as locks and the access systems to certain rooms. CCTV cameras are beginning to be actively used for face recognition and identification of a person who is currently in the room. This entire data stream is transmitted to the university servers where it is processed.

However, IoT also has an increased security problem. Security organization at the university should also take into account the security of endpoints and devices. Interference in their work can cause significant damage to the entire infrastructure. IoT emphasizes the need to focus on cyber resilience – the ability to continue transformation effectively in conditions of increasing threats from national states, criminals, competitors and insiders. These risks include:

- The increasing use of IoT technologies both at the university and by related stakeholders, which leads to the fact that control over data safety is almost absent;
- Constant IoT devices size reduction, which makes it difficult to identify and control them;
- Vulnerability of interrelated IoT devices, which may lead to data interception or data integrity failure;
- Attacks that can interrupt key systems and disrupt operation.

For the cyber resilience achievement, the university should start with a thorough assessment, diagnostics of all the IoT-related assets, which exist within operations, focusing on access control tools and techniques, IoT devices control during their life cycle and providing an active response to incidents.

Continuous monitoring of the devices and the traffic condition of the network is crucial moment of attacks or misconducts identifying. Hackers usually act according to a certain algorithm – kill chain. This classification was proposed by a company «Lockheed Martin» for intrusion detection and prevention. The cybercrime chain consists of seven steps that help which help analysts to understand hacker methods, tools and procedures. The goal of incident response is to identify and stop an attack as early as possible in the cybercrime chain. The sooner the attack is stopped, the less damage will be done and the less the hacker can learn about the target network. The cybercrime chain indicates what actions a hacker must take to achieve his goal, see Fig.1.

If a hacker is stopped at any stage, the chain of attack will be broken. Chain breaking means that a protector managed to successfully repel the hacker's attack. Attackers achieve success if they manage to get to the seventh stage.

Reconnaissance attack: an attacker performs research, gathers analytics, and chooses targets. Based on this data, a hacker can determine whether to take up an attack. Any open access information can help determine what, where and how to attack. There is a great deal of open access information, especially when it comes to large organizations,

including news articles, websites, conferences, and public network devices. Ever-growing amounts of information about employees are available on social networks.

Figure 1. Conditionally-logical representing of a possible cyberattack

The attacker selects targets that have been forgotten or have not been protected, as these objects are more likely to be penetrated or broken. All information obtained by the attacker is analyzed in order to determine its importance, as well as to understand whether it reveals possible additional sources of income from the attack.

The goal of the next phase is to develop weapons against specific target systems within the organization, using information obtained through a reconnaissance attack. To develop these weapons, the designer takes advantage of the resource vulnerabilities that have been discovered and builds them into a tool that can be deployed. After using this tool, the hacker is expected to achieve his goal of gaining access to the target system or network, which reduces the performance of that system (or the entire network). An attacker will continue to examine the network and resource protection in order to identify additional vulnerabilities, gain control over other resources, or deploy new attacks.

It's not difficult to choose the attack weapons. An attacker needs to see what attacks can be used against the vulnerabilities found. There are many off-the-shelf attacks that have been well tested. One problem is that because these attacks are so well known, it is likely that defenders are familiar with them as well. It is often more effective to use an as-yet-unknown attack that eludes detection tools. An attacker might decide to develop a weapon of his own that is specifically designed to prevent detection tools using the information he has gained about the network and systems.

At the delivery stage the weapon is transferred to the target system using a delivery vector. This can be done through a website, removable USB storage devices or an email attachment. If the weapon is not delivered, the attack will fail. To increase the chances of useful data delivering, an attacker will use several different methods, including communications encryption, providing the code with a type of legitimate program or code masking. Security sensors are so sophisticated that they will inevitably recognize the code as harmful unless changes are made to it to avoid detection. The code can be changed to appear harmless, however, it will continue to perform the required actions, even though it may take longer to complete.

After the weapon has been delivered, the attacker uses it to hack the system in the vulnerable spot and gain control over the target system. The most common targets for exploits are applications, operating system vulnerabilities and users. The attack organizer needs to use an exploit that allows him to achieve the desired effect. This is very important because if the wrong exploit is used, it is clear that the attack will not work, and unwanted side effects such as denial of service or multiple system reboots will draw unnecessary attention, allowing cybersecurity analysts to easily gain insight into the attack and the hacker's intentions.

Just during injection a hacker creates a security hole to ensure constant access to the target. In order

to maintain this hole it is important that remote access does not show itself in any way for cybersecurity analysts or users. The method should remain unseen after scanning performed by means of antivirus and reboot the computer necessary for the hole to operate. This continuous access can also provide automatic communication, which is especially effective when several communication channels are needed to control a botnet.

The next stage goal is to establish management and control over the target system. Broken hosts are usually taken off the network and connected to the controller on the Internet. This is because malware requires manual interaction to exfiltrate data from the network. The last stage of the cybercrime chain describes the attacker's achieving goal. This could be data theft, DDoS attacks, or using a broken network to generate and send spam. At this stage, the attacker is already deeply rooted in the organization's system, hiding his actions and covering his tracks. Removing a hacker from the network is extremely difficult.

Considering this information, the information security analyst advises the systems engineer and the security engineer on how to create security rules on the computer network and monitoring systems for different network segments.

First, we will consider the approaches in the architecture of a university computer network to ensure the security of its end devices at the L2-L4 level. It is necessary to know that there are two main directions of attack – external and internal. If the attacks from the outside are possible and specialists try to respond to them adequately, then internal ones are rather painful for the whole university. Why does this happen? The answer lies in the network general availability. Students and lecturers can generate traffic, which is not tracked. Downloaded programs from torrent trackers, phishing sites browsing, mail with rootkits and other types of threats left their fingerprints on internal personal computers located in university buildings. If to track all traffic over the network, one can see that there is no way to influence any rules on L2 traffic. Of course you can configure port security and bind a computer to the PC to the switch ports rather hard, configure ACL for L3 / IR, however to track traffic or to inspect packages is impossible.

One of the solutions is to apply an approach Zone Base Firewall (ZBE) on the edge router, see Fig. 2. This makes it possible to check traffic at L3-L4 levels, reduces the number of descriptions of traffic and network rules. This releases resources for packages processing.

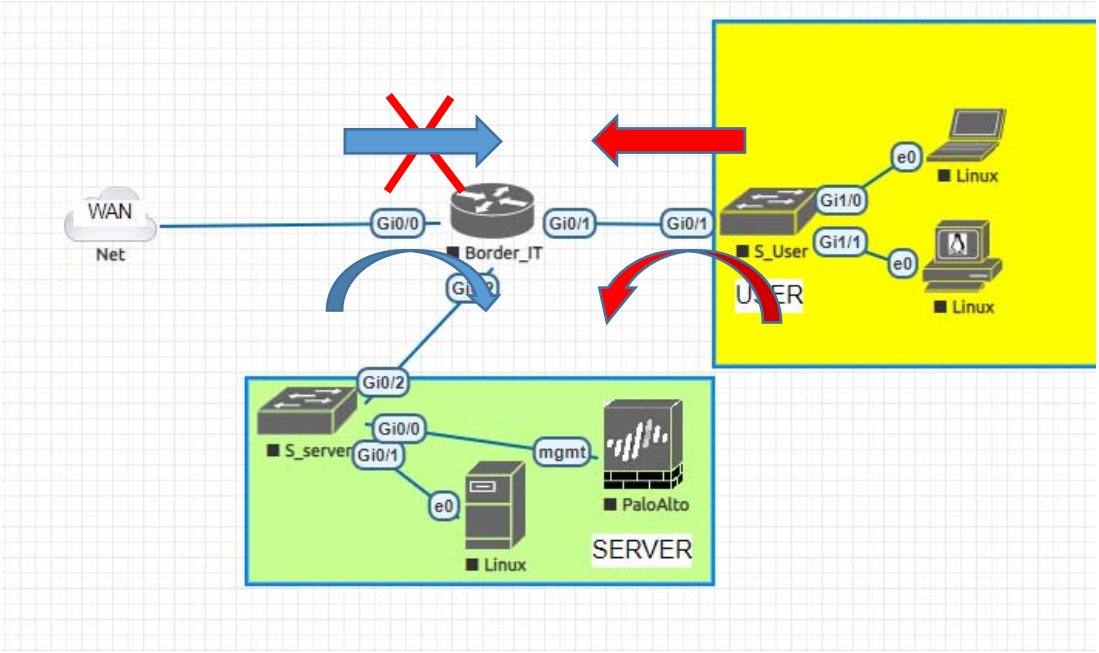

Figure 2. ZBF application example

Fig. 2 shows an approach to using ZBF. First of all, it should be noted that the server segment must be allocated to the demilitarized zone, which is another rule in ensuring network security. To implement ZBF, it is necessary to define the zones to which the corresponding interfaces belong.

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

Links directed to the ISP side are referred to external channels and they must be marked as external (WAN – mark in the figure). Ports connected to users belong to the user segment – User. There is also a server software segment. The traffic that is initiated from the user segment to the

The response from the training portals will go through the router. The advantage of using this approach is that the created session passes only matching traffic. Data are written to a log file. Traffic from outside to the server segment is also allowed. Students will get access to the learning portal from home. Accordingly, such traffic will also be monitored, and if anomalies are detected, the network from which illegal actions are carried

Internet will go through the router, which in turn will remember the session and check the traffic that goes through it. That is, the response to the initialized request will flow on Wednesday to the user segment. The situation is the same when the user enters the server segment.

out is blocked. As for the server segment, it will not be able to enter any of the previously described zones, see fig. 3. This ensures the safety of local users from possible threats from the server segment (in case of servers breaking and infection), as well as their access to the Internet or attacks on the provider.

.

```
Number of Established Sessions = 6
Established Sessions
  Session 3EFE71C0 (172.16.201.139:58135)=>(51.105.249.228:443) tcp SIS_OPEN/TCP_ESTAB
    Created 00:46:54, Last heard 00:26:42
    Bytes sent (initiator:responder) [2436:5125]
  Session 3EFEB0C0 (172.16.201.139:58136)=>(64.233.162.188:443) tcp SIS_OPEN/TCP_ESTAB
    Created 00:46:53, Last heard 00:00:23
    Bytes sent (initiator:responder) [903:4515]
  Session 3EFEA640 (172.16.201.139:58183)=>(8.8.8.8:443) tcp SIS_OPEN/TCP_ESTAB
    Created 00:03:49, Last heard 00:00:04
    Bytes sent (initiator:responder) [1039:1772]
  Session 3EFDDB40 (172.16.201.139:58184)=>(172.217.16.3:443) tcp SIS_OPEN/TCP_ESTAB
    Created 00:03:49, Last heard 00:00:03
    Bytes sent (initiator:responder) [1127:1581]
  Session 3EFEB440 (172.16.201.139:58187)=>(8.8.8.8:443) tcp SIS_OPEN/TCP_ESTAB
    Created 00:01:47, Last heard 00:00:16
    Bytes sent (initiator:responder) [1038:1772]
  Session 3EFDE940 (172.16.201.139:58188)=>(216.58.215.66:443) tcp SIS_OPEN/TCP_ESTAB
    Created 00:01:46, Last heard 00:00:16
    Bytes sent (initiator:responder) [1339:2498]
```

Figure 3: Example of inspecting packets passing university edge route

Computer infrastructure security development doesn't stop at just one approach. So, at the edge router of the net technologies of network addressing modification and ports forwarding to internal addresses are applied. It is also one of the protection elements. However, this approach does not completely close the OSI model in terms of the security of the higher education establishment, if we take into account the model of the killer cyber-chain.

Since IoT devices mainly work with web servers built on different technologies, it is necessary to think over the protection that will cover the L5-L7 level of OSI model. One approach is to use the Web Application Firewall, further – WAF. The WAF itself is a collection of monitors and filters designed to detect and block network attacks on web applications. WAF is referred to the application layer of the OSI model.

The web application can be protected by the application developers without the use of WAF. This requires additional development costs, for example information security department salary. WAF has incorporates the ability to protect against all known information attacks, that allows delegating its protection function.

Since the work of the firewall significantly delays the speed of traffic to the network, traffic is being checked for malware. Such control points should be placed with sufficient care. For example, in Fig. 4 the scheme of IoT devices integration into the university computer network is presented. The network itself is divided into two segments. One part is conditionally considered a demilitarized zone, since the server farm is located there. Another part of the network is related to users, classrooms and laboratories. It can be seen from the diagram that in the part of the user network, all devices are connected to one switch. This approach allows allocating the corresponding traffic to a special

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

channel. Therefore, this makes it easy to configure a WAF that is bridged between two switches. This approach allows more precisely configuration the firewall for the type of traffic that the IoT devices generate. At the same time, it does not allow ordinary users to penetrate the IoT network. Such approach enables the elements of artificial intelligence on the WAF to more accurately conduct training in identifying threats and offloads the hardware without loading it with unnecessary traffic.

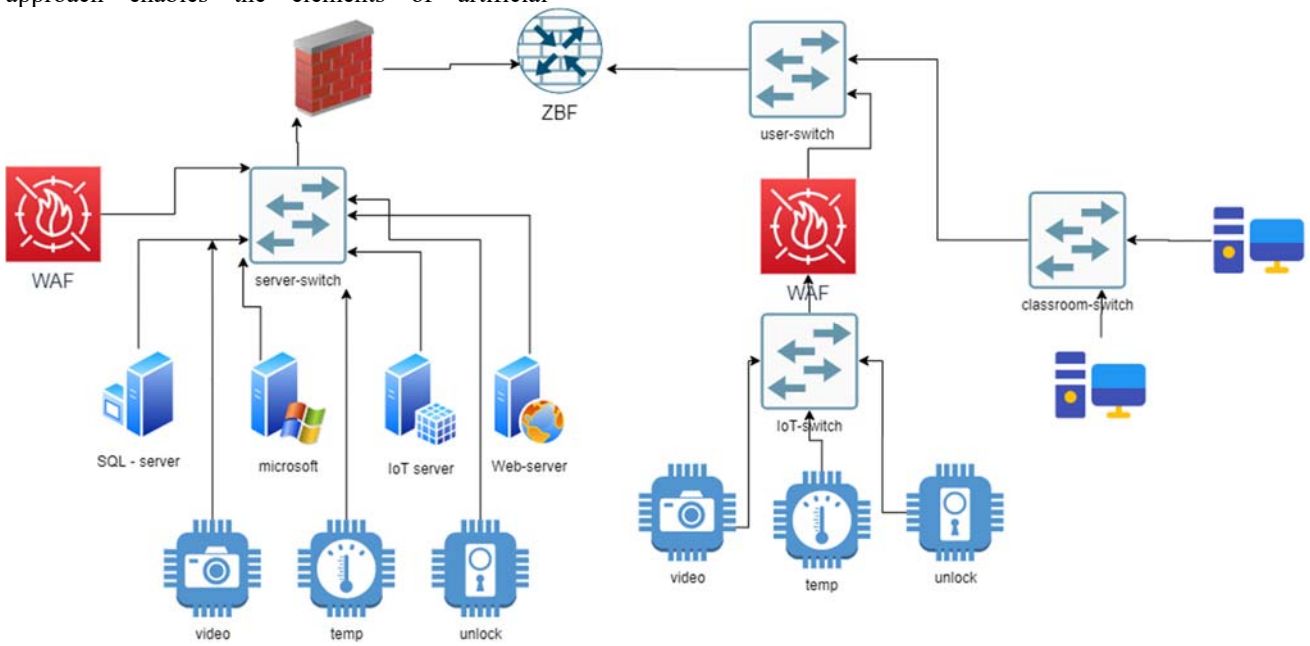

Figure 4: Scheme of IoT devices integration into a university computer network

The server segment has its own specifics. First, there is a hardware firewall that inspects incoming and outgoing traffic. Second is the availability of a server segment switch. In this case, WAF is enabled as a separate user. WAF operates as a passive traffic watcher. In this case, the connection channel is not slowed down as much with the connection speed. The switch port acts as a mirror and all traffic generated is forwarded to the WAF. This allows setting firewall up for deeper threats and hazardous signatures identifying, without limiting of data transmission bandwidth of the channel. IoT devices are physically connected to the same server switch but they are logically placed in a virtual local area network operating according to the priority rules of the IoT server access.

Testing of WAF operation in the proposed network topology was assigned to the ModSecurity program. This software is distributed under a free license and can be customized to suit one's unique needs. Considering the code openness and its application under Linux, it can also be improved and developed according to the identified attacks. There are two options for deploying ModSecurity: deploying directly to a web server, installing as a Reverse Proxy. In the first case, ModSecurity intercepts all requests to the web server on which it is installed: the request from the client is first compared with the filtering rules, and then forwarded for further processing by the web server. ModSecurity can also control web server responses, that is, after the web page is generated, the response is processed by the module and, according to the rules, allows or blocks the passage of responses from the web server.

Installation as a reverse proxy server allows interception requests from web server clients, scan this traffic and redirect to other web servers. Clients can only see the interface of the proxy server and cannot see the web servers hosted behind it. The internal server response is sent through the proxy server.

You can deploy ModSecurity both on a separate dedicated physical and virtual machine. It all depends on the tasks; in our proposed scheme the dedicated physical device will be used. It was preinstalled with Linux OS and Apache web server. For WAF operation you must have your own server

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

to access the database with the ability of remote requests.

5. EXPERIMENTAL STUDY ON A CYBER ATTACK POSSIBILITY

An example of a server deployment is shown below in Figures 5-7.

After the web server Apache installation, you need to install ModSecurity using the apt-get install libapache2-modsecurity command.

```
root@NanoPi-R1:~# apt-get install apache2
Reading package lists... Done
Building dependency tree
Reading state information... Done
The following additional packages will be installed:
  apache2-bin apache2-data apache2-utils libaprl libaprutill libaprutill-dbd-sql
  libaprutill-ldap liblua5.1-0 ssl-cert
Suggested packages:
  www-browser apache2-doc apache2-suexec-pristine | apache2-suexec-custom ufw op
The following NEW packages will be installed:
  apache2 apache2-bin apache2-data apache2-utils libaprl libaprutill libaprutill
  libaprutill-ldap liblua5.1-0 ssl-cert
0 upgraded, 10 newly installed, 0 to remove and 10 not upgraded.
Need to get 1,412 kB of archives.
After this operation, 4,986 kB of additional disk space will be used.
Do you want to continue? [Y/n] y
```

Figure 5: A web server Apache installation

```
root@NanoPi-R1:~#  apt-get install libapache2-modsecurity
Reading package lists... Done
Building dependency tree
Reading state information... Done
The following additional packages will be installed:
  libapache2-mod-security2 libyajl2 modsecurity-crs
Suggested packages:
  lua geoip-database-contrib ruby
The following NEW packages will be installed:
```

Figure 6: ModSecurity installation

For installation accuracy testing let's use the command apachectl -M | grep security. If the installation was successful, the command should output security2_module (shared).

Journal of Theoretical and Applied Information Technology
30th April 2021. Vol.99. No 8

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

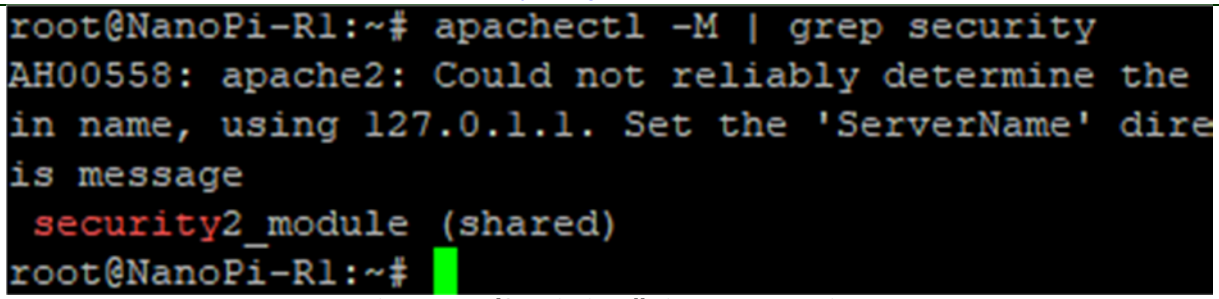

Figure 7. ModSecurity installation accuracy testing

ModSecurity includes a recommended modsecurity.conf-recommended configuration file located in the / etc / modsecurity directory. For this file to work with ModSecurity, you need to rename it using the command mv /etc/modsecurity/modsecurity.conf-recommended /etc/modsecurity/modsecurity.conf.

Further stages of the attack are shown in Fig. 8-12

Figure 8. Configuration files renaming

Using any text editor, edit the contents of the modsecurity.conf file. Change "SecRuleEngine Detection Only" to "SecRuleEngine On", save the changes and exit the text editor, see fig. 9.

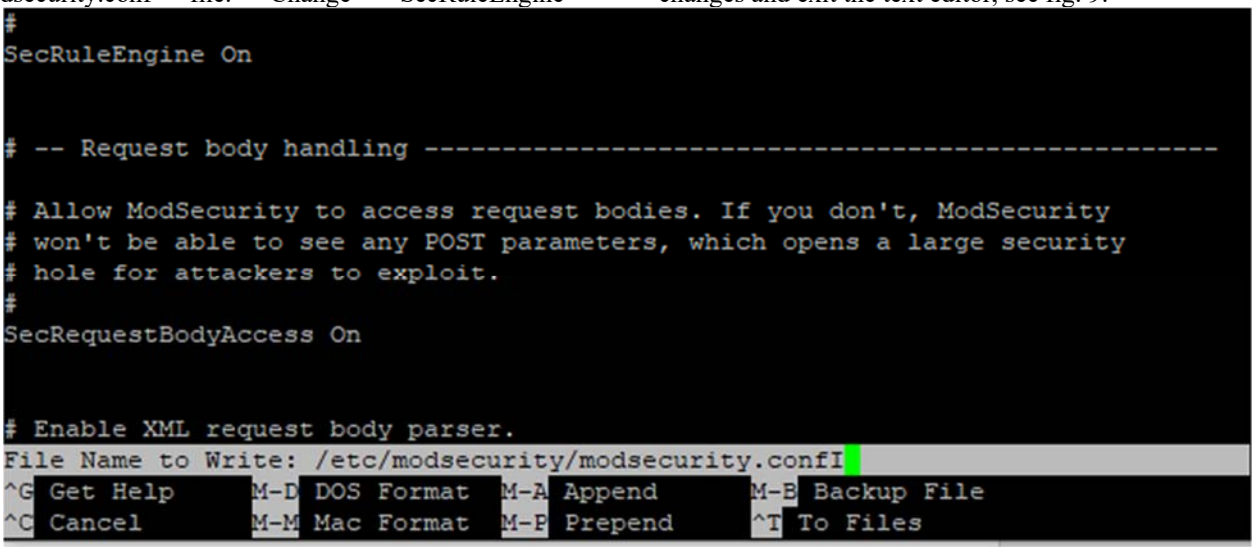

Figure 9. Editing of modsecurity.conf. file

After editing the file, restart the Apache web server, see fig.10.

```
root@NanoPi-R1:~# systemctl restart apache2
root@NanoPi-R1:~# systemctl status apache2
● apache2.service - LSB: Apache2 web server
   Loaded: loaded (/etc/init.d/apache2; bad; vendor preset: enabled)
  Drop-In: /lib/systemd/system/apache2.service.d
           └─apache2-systemd.conf
   Active: active (running) since Sat 2021-02-06 18:52:03 UTC; 1min 0s ago
     Docs: man:systemd-sysv-generator(8)
  Process: 23133 ExecStop=/etc/init.d/apache2 stop (code=exited, status=0/SUCCES
  Process: 23156 ExecStart=/etc/init.d/apache2 start (code=exited, status=0/SUCC
   CGroup: /system.slice/apache2.service
           ├─23171 /usr/sbin/apache2 -k start
           ├─23174 /usr/sbin/apache2 -k start
           └─23175 /usr/sbin/apache2 -k start

Feb 06 18:52:00 NanoPi-R1 systemd[1]: Starting LSB: Apache2 web server...
Feb 06 18:52:00 NanoPi-R1 apache2[23156]:  * Starting Apache httpd web server ap
Feb 06 18:52:01 NanoPi-R1 apache2[23156]: AH00558: apache2: Could not reliably d
Feb 06 18:52:03 NanoPi-R1 apache2[23156]:  *
Feb 06 18:52:03 NanoPi-R1 systemd[1]: Started LSB: Apache2 web server.
lines 1-18/18 (END)
```

Figure 10. Web-server restarting

ModSecurity comes with Core Rule Set. CRS is aimed at meb-applications protecting from a wide range of attacks (including OWASP Top Ten), with a minimum false response. CRS rules are stored in the /usr/share/modsecurity-crs directory.

```
root@NanoPi-R1:~# ls -l /usr/share/modsecurity-crs/
total 44
drwxr-xr-x 2 root root  4096 Feb  6 17:12 activated_rules
drwxr-xr-x 2 root root  4096 Feb  6 17:12 base_rules
drwxr-xr-x 2 root root  4096 Feb  6 17:12 experimental_rules
drwxr-xr-x 2 root root  4096 Feb  6 17:12 lua
-rw-r--r-- 1 root root 13809 Oct 25  2014 modsecurity_crs_10_setup.conf
drwxr-xr-x 2 root root  4096 Feb  6 17:12 optional_rules
drwxr-xr-x 2 root root  4096 Feb  6 17:12 slr_rules
drwxr-xr-x 8 root root  4096 Feb  6 17:12 util
root@NanoPi-R1:~#
```

Figure 11. A set of basic CRS rules

For further work, a set of rules will be used, drawn up accordingly for the needs of corporate university network protection and IoT devices protecting. Remove default rule set with the rm -rf/usr/share/modsecurity-crs command. Create a new directory in the Apache directory using the command, see fig. 12:

```
root@NanoPi-R1:~# mkdir /etc/apache2/modsecurity.d
root@NanoPi-R1:~# cd /etc/apache2/
root@NanoPi-R1:/etc/apache2# ls
apache2.conf     conf-available  envvars  mods-available  mods-enabled  sites-available
apache2.conf.in  conf-enabled    magic    modsecurity.d   ports.conf    sites-enabled
root@NanoPi-R1:/etc/apache2#
```

Figure 12. Creating a directory modsecurity

Journal of Theoretical and Applied Information Technology
30th April 2021. Vol.99. No 8

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

Load the basic set of Modsecurity rules. Copy the sample configuration file from the loaded rule set with the command cp crs-setup.conf.example crs-setup.conf.

We edit the Apache configuration file as follows, see fig. 13.

```
<IfModule security2_module>
        SecDataDir /var/cache/modsecurity
        IncludeOptional /etc/modsecurity/*.conf
        IncludeOptional "/usr/share/modsecurity-crs/*.conf
        IncludeOptional "/usr/share/modsecurity-crs/rules/*.conf
 </IfModule>
File Name to Write: /etc/apache2/apache2.conf
^G Get Help      M-D DOS Format    M-A Append        M-B Backup File
^C Cancel        M-M Mac Format    M-P Prepend       ^T To Files
```

Figure 13. Editing the Apache configuration file

Check the Apache configuration and restart the web server. To test the operation of WAF after the previous settings, we will test the resources on the server segment.

On a remote computer, run the following command to test ModSecurity for XSS attacks:url http://192.168.1.251/?q="><script>alert(1)</script>'. In this case, we will receive a response from the 403 Forbidden server.

<!DOCTYPE HTML PUBLIC "-//IETF//DTD HTML 2.0//EN">
<html><head>
<title>403 Forbidden</title>
</head><body>
<h1>Forbidden</h1>
You don't have permission to access /
on this server.

<hr>
<address>Apache/2.4.18 (Ubuntu) Server at 192.168.1.251 Port 80</address>
</body></html>

After that, let's carry out a simple SQL injection attack. We enter the following URL into the address bar of the browser: http://192.168.1.251/?id=3%20or%20%27a%27=%27a%27 and get, see fig. 14:

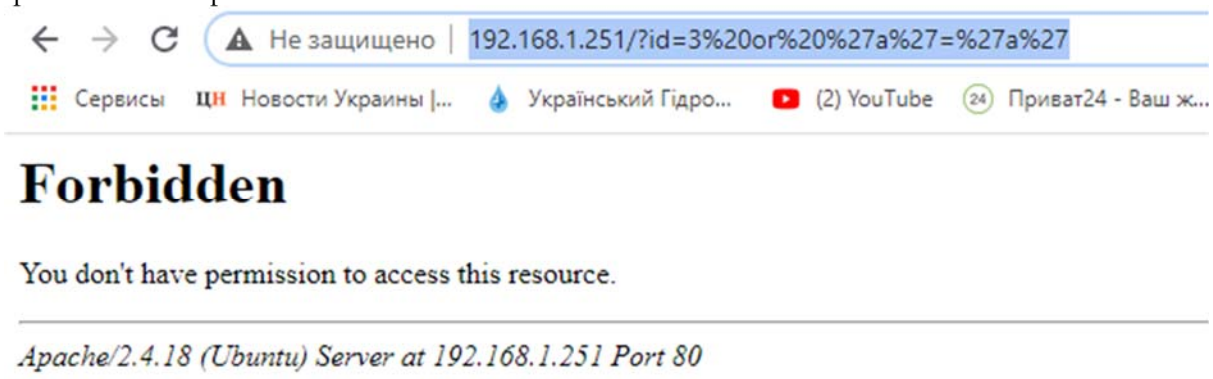

Figure 14. Successful protection against simple SQL injection

In the audit log /var/log/apache2/modsec_audit.log you can see the following information, which means that ModSecurity blocked this attack using OWASP v3.3.0, see Fig. 15.

Figure 15. Information from the audit log

6. DISCUSSIONS OF THE EXPERIMENTAL RESEARCH RESULTS

This approach of integration and protection will be further formalized in a mathematical model that allows formalizing a mathematical approach to determining the vulnerabilities of the university network. It is worth pointing out that IoT devices will develop rather quickly and enter our life deeper and deeper. This is especially true for higher educational establishments. Therefore, in our future works we will develop this approach in our research.

In further research, it is planned to work on improving the methodology for ensuring protection and monitoring of the university infrastructure, as well as improvement of the software part for the identification of possible threats, their identification and implementation of artificial intelligence elements into the work of WAF firewalls to identify threats directed to the Internet of Things devices.

7. CONCLUSIONS

The development of computer networks in modern educational institutions runs away. Every year new challenges are emerging to ensure the security of data and the very end users. With the advent of the Internet of Things (IoT) this problem has become quite acute for network engineers and cyber analysts. In increasing frequency there are illegal actions regarding interference in the operation of the network itself and the use of users' devices for criminal purposes. Various distributed attacks, SQL injections and identity theft are becoming more complex. Considering the growth of both the network infrastructure itself and the IoT devices, there is a need for their protection, especially when it comes to the computer network of a higher establishment, where usually little attention is paid to the full protection of the infrastructure, and with the integration of IoT devices, there can be quite a lot of such possible gaps.

This article is an attempt to disclose practical approaches to the design and implementation of a computer network of an educational establishment (in case of a university), which in recent years are increasingly beginning to suffer from outside interference. Possible attacks on the university infrastructure, as well as the possibility of attacks and interference in the operation of IoT devices based on the approach of a kill chain of a possible cyberattack have been analyzed.

The paper considers the possibility of using a web application firewall and corresponding software for security and incident response at the L5-L7 OSI level in such networks. Preliminary testing of the network for the ability to respond to both L3-L4 attacks, using standard firewall capabilities, as well as with the response to intervention at the upper levels of the OSI L5-L7 model (SQL injection, distributed DDoS, bot attacks of the networks) has been carried out. The results have been summarized and further directions of research, based on improving the group security policy for higher educational establishments, development of security infrastructure for IoT devices and the ability of quick response to non-standard attacks, have been identified.

Coming to a conclusion on the above material, one can say that the need to integrate IoT devices into the university IT structure as economically as possible, protection of such devices become very important, because they can give attackers information about the personal data that may be stored on digital university media.

REFERENCES:

[1] Abomhara, M., & Køien, G. M. (2015). Cyber security and the internet of things: vulnerabilities, threats, intruders and attacks. *Journal of Cyber Security and Mobility*, 65-88.

[2] Weber, R. H., & Studer, E. (2016). Cybersecurity in the Internet of Things: Legal aspects. *Computer Law & Security Review*, 32(5), 715-728.

[3] Zhao, S., Li, S., Qi, L., & Da Xu, L. (2020). Computational intelligence enabled cybersecurity

for the internet of things. *IEEE Transactions on Emerging Topics in Computational Intelligence*, 4(5), 666-674.

[4] Sani, A. S., Yuan, D., Jin, J., Gao, L., Yu, S., & Dong, Z. Y. (2019). Cyber security framework for Internet of Things-based Energy Internet. *Future Generation Computer Systems*, 93, 849-859.

[5] Lu, Y., & Da Xu, L. (2018). Internet of Things (IoT) cybersecurity research: A review of current research topics. *IEEE Internet of Things Journal*, 6(2), 2103-2115.

[6] Zavgorodniy, VV, Drozdova, EA, & Kozel, VM (2020). Analysis of security problems Iot devicev. *Bulletin of Kherson National Technical University*, (4 (75)). Pp. 59-66.

[7] Trokhimenko, DV, & Kurdecha, VV (2019). Data protection on the Internet of Things. *International scientific and technical conference 228 "Radio fields, signals, devices and systems"*, p. 228-230.

[8] Akhmetov, B., Lakhno, V., Yerkeldessova, G., Sarzhanov, T., Issaikin, D. Simulation model of gprs channels operation as a part of the railway traffic coordination system (2019) *International Journal of Electronics and Telecommunications*, 65 (3), pp. 485-490.

[9] Akhmetov, B., Lakhno, V., Oralbekova, A., Kaskatayev, Z., Mussayeva, G. Automated self-trained system of functional control and state detection of railway transport nodes (2019) *International Journal of Electronics and Telecommunications*, 65 (3), pp. 491-496.

[10] Borowik, B., Karpinskyy, M., Lahno, V., Petrov, O. Machines Moore and Mealy (2013) *Intelligent Systems, Control and Automation: Science and Engineering*, 63, pp. 143-171.

[11] Borowik, B., Karpinskyy, M., Lahno, V., Petrov, O. Binary Arithmetic (2013) *Intelligent Systems, Control and Automation: Science and Engineering*, 63, pp. 19-35.

[12] Borowik, B., Karpinskyy, M., Lahno, V., Petrov, O. Latches, Flip-Flops, Counters, Registers, Timer, Multiplexer, Decoder, Etc. (2013) *Intelligent Systems, Control and Automation: Science and Engineering*, 63, pp. 101-141.

[13] Borowik, B., Karpinskyy, M., Lahno, V., Petrov, O. Boolean Algebra (2013) *Intelligent Systems, Control and Automation: Science and Engineering*, 63, pp. 45-49.

[14] Borowik, B., Karpinskyy, M., Lahno, V., Petrov, O. Basic Logical Functions and Gates. Logic Design (2013) *Intelligent Systems, Control and Automation: Science and Engineering*, 63, pp. 51-73.

[15] Alimseitova, Zh., Adranova, A., Akhmetov, B., Lakhno, V., Zhilkishbayeva, G., Smirnov, O.A. virtual cloud resources (2020) *Journal of Theoretical and Applied Information Technology*, 98 (21), pp. 3334-3346.

[16] Lakhno, V.A., Kartbayev, T.S., Turginbayeva, A.A., Alimseitova, Z.K., Beketova, G.S. Analysis of existing and development prospects of decision support systems for evaluating investment projects in the field of enterprise digitalization (2020) *International Journal of Advanced Trends in Computer Science and Engineering*, 9 (5), pp. 8533-8539.

[17] Lakhno, V.A., Kasatkin, D.Y., Kartbayev, T.S., Togzhanova, K.O., Alimseitova, Z.K., Tussupova, B.B. Analysis of methods and information technologies for dynamic planning of smart city development 2020) *International Journal of Advanced Trends in Computer Science and Engineering*, 9 (5), статья № 83, pp. 7496-7505.

[18] Sahun, A.V., Lakhno, V.A., Kravchuk, P.Y., Kosenko, S.S., Kisiliuk, E.M. Elliptic curves in modern cryptographic systems (2020) *International Journal of Advanced Trends in Computer Science and Engineering*, 9 (4), статья № 259, pp. 5949-5955.

[19] Lakhno, V., Kryvoruchko, O., Desiatko, A., Blozva, A., Semidotska, V. Development strategy model of the informational management logistic system of a commercial enterprise by neural network apparatus (2020) *CEUR Workshop Proceedings*, 2746, pp. 87-98.

[20] Kalizhanova, A., Akhmetov, S., Lakhno, V., Wojcik, W., Nabiyeva, G. Optimization model of adaptive decision taking support system for distributed systems cyber security facilities placement (2020) *International Journal of Electronics and Telecommunications*, 66 (3), pp. 493-498.

[21] Lakhno, V.A., Kasatkin, D.Y., Blozva, A.I., Kozlovskyi, V., Balanyuk, Y., Boiko, Y. The Development of a Model of the Formation of Cybersecurity Outlines Based on Multi Criteria Optimization and Game Theory (2020) *Advances in Intelligent Systems and Computing*, 1295, pp. 10-22.

[22] Lakhno, V., Malyukov, V., Kasatkin, D., Vlasova, G., Kravchuk, P., Kosenko, S. Model for Choosing Rational Investment Strategies, with the Partner's Resource Data Being Uncertain (2020) *Advances in Intelligent Systems and Computing*, 1295, pp. 332-341.

[23] Lakhno, V., Malyukov, V., Akhmetov, B., Gerasymchuk, N., Mohylnyi, H., Kravchuk, P. Decision Support Model for Assessing Projects by a Group of Investors with Regards of Multi-factors (2020) *Advances in Intelligent Systems and Computing*, 1225 AISC, pp. 1-10.

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

[24] Lakhno, V.A., Malikov, V.G., Kasatkin, D.Y., Blozva, A.I., Saiko, V.G., Domrachev, V.N. Computer-Based Support for Searching Rational Strategies for Investors in Case of Insufficient Information on the Condition of the Counterparty (2020) *Advances in Intelligent Systems and Computing,* 1225 AISC, pp. 120-130.

[25] Lakhno, V., Malyukov, V., Mazur, N., Kuzmenko, L., Akhmetov, B., Hrebeniuk, V. Development of a model for decision support systems to control the process of investing in information technologies (2020) *Eastern-European Journal of Enterprise Technologies,* 1 (3), pp. 74-81.

[26] Valeriy, L., Volodymyr, M., Olena, K., Mykola, T., Alyona, D., Tetyana, M. Model of Evaluating Smart City Projects by Groups of Investors Using a Multifactorial Approach (2020), *Communications in Computer and Information Science,* 1193 CCIS, pp. 13-26.

[27] Akhmetov, B. et al. Adaptive Decision Support System for Scaling University Cloud Applications, (2021), *Studies in Systems, Decision and Control,* 337, pp. 49-60.

[28] Valeriy, L. et al. Computer support system for choosing the optimal managing strategy by the mutual investment procedure in smart city, (2020), *Advances in Intelligent Systems and Computing,* Vol. 1194, pp. 278-287.

[29] Mailybayev, Y., Umbetov, U., Lakhno, V., Omarov, A., Abuova, A., Amanova, M., Sauanova, K. Development of mathematical and information support for solving prediction tasks of a railway station development (2021) *Journal of Theoretical and Applied Information Technology*, 99 (3), pp. 583-593.

[30] Lakhno, V., Akhmetov, B., Adilzhanova, S., Blozva, A., Svitlana, R., Dmytro, R. The use of a genetic algorithm in the problem of distribution of information security organizational and financial resources (2020) ATIT 2020 - Proceedings: 2020 *2nd IEEE International Conference on Advanced Trends in Information Theory*, № 9349310, pp. 251-254.