How to use cyber kill chain model to build cybersecurity?

Ireneusz Tarnowski

Wroclaw Centre for Networking and Supercomputing, Wroclaw University of Science and Technology, Wybrzeze Wyspianskiego 27, 50-370 Wroclaw, Poland

e-mail: mailto:ireneusz.tarnowski@pwr.edu.pl

Paper type

Case study

Abstract

The term “Cyber Kill Chain” has been widely used by the security community to describe the different stages of cyber attacks. This model is intrusion-centric, which was the focus of cyber security when it was created. They can be used for protection of an organization's network. The stages are: Reconnaissance, Weaponization, Delivery, Exploit, Installation, Command & Control, Actions.

When combined with advanced analytics and predictive modeling, however, the cyber kill chain becomes critical for inside out security. With the above breakdown, the kill chain is structured to reveal the active state of a data breach. User behavior analytics brings advanced threat intelligence to every stage of the kill chain – and helps prevent and stop ongoing attacks before the damage is done.

The WASK network connects the academic institutions of Wrocław, providing them with access to Polish national network PIONIER and European network GÉANT2. The article describes how to prepare organization or metropolitan area network (MAN) to cyber attack. WASK team use a modern approach to cybersecurty in own network and implement security policy on the edge of network. All internal services are protected using application firewall (common name „next generation firewall”). Author using methodology based on cyber kill chain implement security policy to increase level of cyber security in network (exactly to defend all central services). Solution which is used, focus on detecting ongoing attacks -- attackers that have already breached your perimeter -- before the damage is done. Instead of analyzing old malware, deploy a breach detection system that automatically detects and analyzes the changes in user and computer behavior that indicate a breach. Mapping security controls and procedures to each stage of the kill chain, WASK security team will develop very detailed, result-oriented security procedures.

Article provides information how to understand kill chain model, how implement security policy to could respond on incident and how should look incident response procedures. All of that is important to build cybersecurity in data center.

Keywords

cybersecurity, network defense, kill chain, incident response, threat detection

1. Introduction

Conventional network defense tools, such as IDS, firewalls and antivirus software, use static knowledge of existing system threats and vulnerabilities. Such approach lets us observe more and more successful computer attacks, which result in spectacular data leaks. The evolution of cybercriminals goals and the use of sophisticated tools means that traditional approaches are no longer sufficient. Network defense techniques using knowledge of opponents, threat modeling, and attack scenarios can significantly reduce the probability of each attempted attack. Using the kill chain model helps to understand the purpose and methods of attack so that the computer incident response team (CERT / CSIRT) can more easily identify participants in the anti-organization campaign and determine the directions and methods of defense. The evolution of current attacks requires changing the defense model to a model built on threat information, focusing not only on vulnerabilities but also on threats. It is important to defend not only the weak elements of the system or the system as one entity, but to defend itself against threats - those known and unknown, in a comprehensive manner, independent of the weakness of the system.

2. How does computer attack look like

In order to understand how a computer attack is conducted and thus be able to react appropriately to each attack, it is necessary to analyze the attack process at every stage of its existence. Each phase of the computer attack is a causal chain, the so-called "Kill chain". The term as well as the names of chain phases are derived from military terminology. An effective attack (which can result in system compromise or data theft) is a chain of events: from the initial identification phase, which aims to get to know the victim, by hacking, the two-way data flow in the computer network, the use of vulnerability, and the infection of the system. control. We can analyze each of these events, gain knowledge and use it to break this chain as early as possible. The deeper we analyze these events, the more we learn from the attackers. Proper detection of the attack becomes the key to defense.

In the computer assault model, the following phases were distinguished:

Reconnaissance
Finding, identifying and choosing a destination, often carried out by scanning the internet, web sites, newsgroups, social media or information (white intelligence).

Weaponization
Preparation of attack tools, such as Trojan horses, explosions and data. This is usually a collection of tools that automate the arming. Place prepared tools in infected files that the victim will use (such as PDFs or Microsoft Office files) when they are delivered.

Delivery
Upload of prepared "attack tools" to the attacked environment, through a pre-prepared attack vector (such as email attachments, web pages, or USB media).

Intrusion, Exploitation
After delivering the "attack tools" to the victim machine, the code is executed in the attacked environment. Most often exploits are vulnerabilities in applications or the operating system of an attacked computer. There are much simpler burglaries that use configuration errors or user unawareness.

Installation
Installing a Trojan horse or so called “backdoor” in the victim's system allows the permanent existence in the attacked environment.

Command and Control
Take control of the infected device. Typically, the compromised computer connects to the Control and Control (C2) computer through a specially created communication channel.

Actions on Objective
It is only at this point that the right action is taken to achieve the objectives. Typically this is a penetration, analysis, collection and copying of data. Alternatively, a burglar may use the compromised computer only as a starting point for further attacks and the location from which the trusted victim network is penetrated.

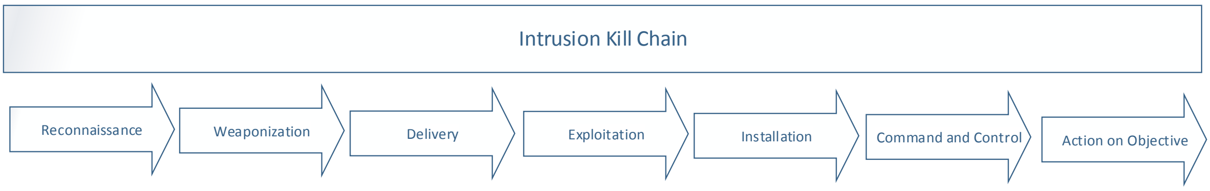


Figure 1. "Kill chain" computer attack

Each cyber-attack phase should be analyzed so that the defender team can determine what action should be taken. They may take different character. First of all, the attack may be detected and it's not that it's going to take place very early in terms of model phases, but rather such a detection can occur in each phase of the attack starting from the run by an attacking reconnaissance activities, ending with the implementation of what was labeled "action". This means that the attacker's target has the most destructive impact on the attacked organization. Steps taken by incident response teams depend on the moment of detection and recognition of the attack.

Unfortunately, the scheme shown in the chain of attack, misleads the potential defender. The problem is the correct presentation of time scale. Now the whole attack can be divided into the preparation phase (Phase 1 Reconnaissance and Phase 2 Arming), Incident Phase (Phase 3 Delivery, Phase 4 Intrusion, Phase 5 Installation) and Active Intrusion Phase (Phase 6 Control and Phase 7 Action). Time to prepare for the attack lasts hours of reconnaissance, and sometimes even months. Then there is an intrusion, understood as the entrance to the attacked infrastructure. It may take up to a few seconds. This stage is the best coordinated and conducted element of the whole attack. The better the preparation, the faster and more effective is the incursion. After successful penetration of the attacked infrastructure, if the attack is not noticed, it is hidden and the intruder's intrusion into the infrastructure of the victim. This stage extends as long as possible, even several months. If the attack goes through all phases, it means that the victim was unable to notice in any way that she was the subject of the attack. This may be due to the very good preparation of the attacker, but often the reason for not detecting the attack is poor preparation of the victim (lack of appropriate monitoring, lack of tools, lack of protective procedures, poor security policy).

At present, more than 90% of attacks start with a random search for a victim (performing a victim search phase). In random attacks, there are also those on a large scale that skip the reconnaissance phase and immediately attempt to break the security of the potential victim, counting on the mistakes he made (wrong configurations, lack of software updates, human factor). These attacks usually start with mass phishing or more sophisticated spear phishing. Attackers "go short," often omitting costly preparation for the attack, they just ask their victim to install malware, hoping that they will succeed. The effectiveness of this method is shocking.

3. Preparation of the defense system

Understanding how a computer attack can give advantage a security team in our organization. First, you can deliberately plan a security architecture to detect attacks and identify where the "site" of your plan is attacking. This will greatly facilitate the selection of defense measures (tools and procedures). The main goal is to break the chain of attack ("kill chain") at any stage, except for the last one, where system compromise and data theft occur.

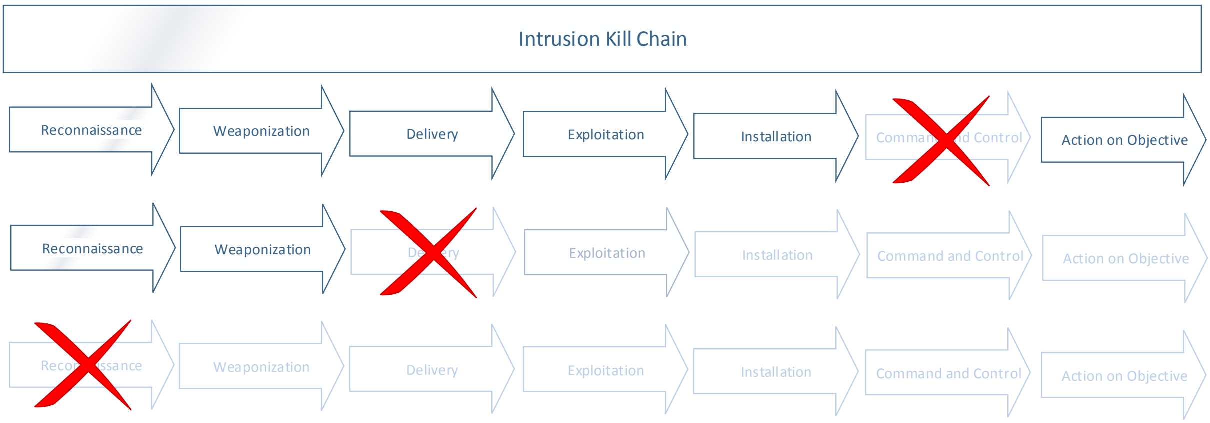


Figure 2. Attack chain "kill chain" - attack detection area and chain break.

In order to be able to interrupt or significantly impede the attack, it is necessary to prepare the infrastructure to take into account security needs already at the design stage. Here you can use the methods of designing security by design and Defense in Depth.

Using knowledge of the aggressor's tactics, you should prepare your infrastructure to counter attacks in the broadest possible range of types and the means that our organization uses. When preparing a defense infrastructure architecture, it is important to set goals for the performance of equipment, procedures, policies and people.

These tasks are:

Detect - Detect an attack. Detecting an attack and correctly diagnosing a scenario is the basis for taking steps to neutralize it. It can be assumed that this is the most important functionality of the security system for defense purposes. HIDS, NIDS, firewalls, antivirus software, log analyzers, network traffic analyzers, integrated event correlation (SIEM) systems, file integrity control, and even well-trained or vigilant computer system user.

Prevention - counteracting attacks. This sentence is intended to prevent an attack. Intrusion Prevention (IPS), scan lock, firewalls, access control lists (ACLs), penetration tests, code obfuscation, custom configurations, vulnerability and availability updates, application whitelist, "sandboxing" and, above all, a well-implemented information security policy.

Disrupt - disrupt the attack. By using some technical solutions you can significantly impede a computer attack, you can technically make the attack less effective or the time to prepare and carry it long enough for the entire operation to become unprofitable for the attacker. Among technical interference methods, the "hardening" of the system should be applied in accordance with the recommendations for the type of system. In addition, you can use computers and network traps (honeypots, honeynets), you can also specify well-matched connection limits (application sessions as well as lower layers of the model - TCP session) or data limits.

Degrade - Degradation of attack. It consists in weakening the power of attack, and consequently its effectiveness. The attack itself is conducted (e.g., denial-of-access attack - DdoS), but by degrading the results to our organization are insignificant. The tools and techniques that can be used to accomplish this task are tarpit, configuration changes to shorten session times (short lead times), policies that impede the inclusion of services (time limitation, limitation for different users).

Deceive - hindering the attack. The deception effect is achieved by introducing the attacker and by forcing the wrong assumptions about the system, which will result in selecting an ineffective attack vector. Deceptive tools include honeypots, obfuscation of application code, or returning incorrect application, server, or configuration information.

Table 1. A list of technical solutions for defense tasks in different stages of cyber-attack.

	Detect	Prevention	Disrupt	Degrade	Deceive
Reconnaissance	IDS HoneyPot Webanaytics	IPS port scanning deny FW ACL	HoneyNet connections limits data limits IPS	Timeout	HoneyPot version obfuscating
Weaponization	Threats information sharing Vulnerability intelligence NIDS	Threats information sharing Pentests Application obfuscation System and application patching Version hidden NIPS	Hardening Version obfuscating	Application obfuscation Unused services disabling	
Delivery	IDS logi FW Network analysis users	Network IPS Firewall Port Knocking ACL change fabric settings network traffic disable Proxy	Hardening In-line AV	Mandatory Integrity	HoneyPot
Exploitation	HIDS logi analiza ruchu anomalia w ruchu	Local sandbox System and application updates	Hardening DEP	Configuration auto rollback	HoneyPot
Installation	HIDS IP Sonar Integrity check Configuration check	App Whitelisting Host IPS Jail (chroot)	Hardening AV	Configuration auto rollback TARPIT	HoneyPot DNS redirect
Command and Control	NIDS SIEM TI Feed	Whitelisting FW ACL	NIPS	QoS	HoneyPot
Actions on Objective	Log analysis				

Explanations to the table:

HIDS	*Host Based Intrusion Detection*
NIDS	*Network Intrusion Detection System*
IPS	*Intrusion Prevention System*
NIPS	*Network-based Intrusion Prevention System*
TI Feed	*Threat Intelligence Feed*
ACL	*Access Control List*
AV	*Antyvirius*
FW	*Firewall*
QoS	*Quality of Service*
HoneyPot	mechanism set to detect, deflect, or, in some manner, counteract attempts at unauthorized use of information systems
HoneyNet	network set up with intentional vulnerabilities; contains one or more honey pots
TARPIT	service that purposely delays incoming connections
DEP	*Data Execution Prevention*
Port Knocking	method of externally opening ports by generating a connection attempt on a set of prespecified closed ports

The list of methods and tools for each task is not closed. The most popular were only listed. Depending on the specifics of the environment, other tools can be implemented, that are important to be effective. For purely technical tools, organizational solutions need to be added, where the most important are trained personnel, procedures and policies, and any knowledge building solution for attackers. Use Threat Intelligences should be taken into action, understood as a study of attack scenarios (techniques and tactics), intelligence and acquisition of information on upcoming and ongoing attacks. This knowledge allows organizations to prepare for attacks, implement security mechanisms by developing new attack scenarios.

Using all these tools, you should model the way they are used to perform tasks in the various phases of the attack. Table 1 provides an overview of the possibilities for implementing various solutions to detect, prevent, disrupt, degrade, or deceive a computer attack in various phases of a computer attack.

4. Detecting an incident and interrupting an attack chain

Depending on the moment of the incident, appropriate steps are taken. Most computer attacks are carried out according to a well-known scenario. At present, 133 scenarios of attacks (TT & CK - Tactics, Techniques & Common Knowledge) have been defined. A security analysis based on information from the defense systems (all implemented mechanisms) determines the occurrence of the incident and defines immediately the attack phase in which the incident was detected. If it is one of the late phases of attack (e.g., Command and Control, fig. 3), then beyond the steps of the incident handling procedure (e.g., stopping, limiting, recovering), it analyzes how far the attack has taken place. The analysis must answer the questions:

- why the attacker reached such a remote place,
- what elements (devices, procedures) of our infrastructure participated in the attack,
- which element should work and protect us in this attack, but that did not happen.

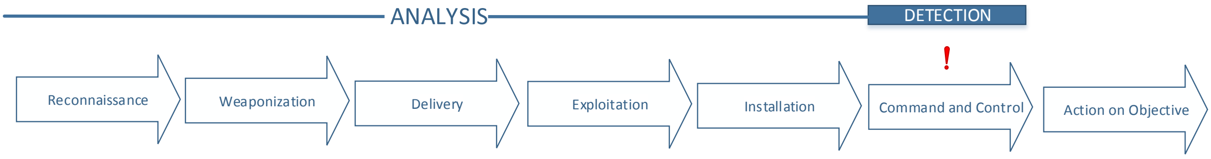


Figure 3. Detection on Incident Control (C2)

Detecting the incident and analyzing it at a late stage that will assess the effectiveness of the cybernetic defense line. It is very important to understand how malware passed the defense line. Most often it will be information about the weaknesses of our system. These places were noticed (mostly during the Reconnaissance) by the aggressor who decided to use them. It is worth strengthening these places (e.g. changing security policy to some extent, improving device configuration, updating or manually writing signatures for devices that detect or seal network access). Looking at the event in the context of the motive and purpose of the attacker will help us to look at our organization from the aggressor's point of view. We will see what we have valuable resources and we will assess whether we protect them properly. Often it turns out that we do not see potential targets of attacks. For each incident it is necessary to answer the question "*How close was the break-in?*", "*How close was the attacker to achieve the goal?*"

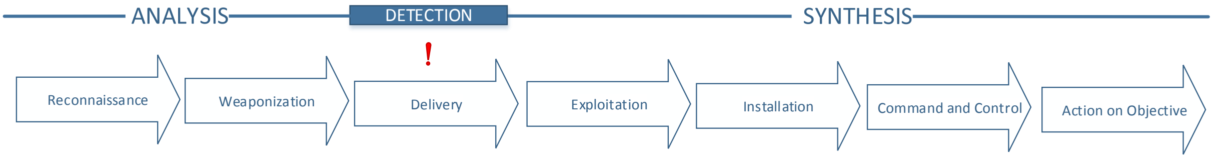


Figure 4. Detection at Delivery stage

When an attack is detected at an early stage (the most common and easiest thing to do in the Delivering phase), it is necessary to analyze what happened as well as to detect it at a later stage, but additionally to do the synthesis. This is to know the next steps of the aggressor and the methods that he wants to use for hacking and installing in the system. Such synthesis after build knowledge of the tactics and tools of the opponent. This knowledge will allow us to provide security protection to defend us from this attack if malicious software is effectively delivered in another, undetected way. During analysis and synthesis, you should determine the attack vector, find vulnerabilities that undermine our infrastructure, and gather the maximum amount of information about the attacker. Often, low level malware analysis is required. This information is used to define the Indicator of Compromise (IoC), which can improve your defense line.

5. Implementation

5.1. Introduction

The Wroclaw Centre for Networking and Supercomputing (WCNS) is a unit of Wroclaw University of Science and Technology with an intercollegiate character. Its main tasks are:

- operation and development of Wroclaw Academic Computer Network (WASK),
- operation and development of high power computers (HPC);
- exploitation and development of network information services for all universities and research institutes in Lower Silesia.

The WASK network connects Wroclaw universities and institutes by providing them with access to the PIONIER national network and the European GÉANT2 network. The area of action of Wroclaw Centre for Networking and Supercomputing is Lower Silesian Voivodeship. The organizational and operational headquarters are located in Wroclaw, where the WCNS Data Center is also located. The Center consists of computing clusters (including Bem and Nova clusters) and service server clusters, private clouds, and resources.

Due to the growing real threats of cyber-attacks, the implementation of protection mechanisms against known and unknown threats has been implemented. Selected advanced solution:

- is an application firewall,
- has features of IPS system,
- realizes the functionality of anti-virus software,
- can control packets in 7 layers (DPI - Deep Package Inspection),
- can analyze encrypted traffic (SSL Inspection),
- will provide total network protection by centralizing workstation (VPN) connections.

These requirements stem from analyzing scenarios of attacks on the computer network and resources of the WCNS Data Center. The attack and defense analysis presented in the previous chapters was used so that the implemented solution was effective and flexible. Multifunctionality and flexibility have been exposed because of the need to work effectively in the long run. They were striving to be able to model and implement protection against threats that were not known at the time of implementation.

5.2. The way of realization

All resources processed in the WCNS Data Center are protected against cyber-attacks. For this purpose, a cluster of high availability and high performance appliances has been implemented, which apply the Application Firewall along with anti-virus protection modules (which include functions of the AV anti-virus system and protection against DLP data leakage). Security policies have been implemented where, apart from the traditional division into security zones (division of networks into segments and regulation of the flow of information between these zones), policies have been implemented that directly address the task of detecting and interrupting an attack. A number of extended policies related to the "Death Chain" have been developed and implemented. These are:

1. Reconnaissance
   - inspection of network traffic, detection and prevention of port scanning,
   - policy to detect redirects to banned sites (URL filtering).

2. Weaponization
3. Delivery
   - inspection of network traffic (including SSL) and blocking of applications that are considered risky,
   - protection policy for all endpoints included in the infrastructure (VPN),
   - blocking of communication with suspicious and risky URLs (URL filtering);
   - blocking the ability to send known exploits and malware, using a variety of protection mechanisms such as IPS, antimalware, antiCnC, sinkholing, DNS traffic monitoring, files blockade.
   - policy to block known and unknown threats through online analysis (WildFire).

4. Intrusion, Exploitation
   - policy to block known and unknown threats through online analysis (WildFire),
   - application control policy for accessing unknown applications and tools (Application Whitelisting).

5. Installation
   - protection against local escalation of permissions on endpoint devices connected to the central firewall, protection against theft of sensitive data (e.g. passwords),
   - policy of creating safety zones with strictly controlled access rights and monitoring traffic between zones and inside the zone (realization of the Zero-Trust model),
   - application control policy for accessing unknown applications and tools (Application Whitelisting).

6. Command and Control
   - blocking of send communications to the server Command and Control (C2),
   - blocking of communication with suspicious and risky URLs (URL filtering),
   - blocking new attack techniques, by detecting application types independently of the port,
   - redirecting suspicious network traffic to local traps and analysis of systems malware (honeypots),
   - building a database of dangerous addresses and domains to protect other devices by controlling DNS queries.

7. Actions on Objective

   - blocking of send communications to the server Comand and Control (C2),
   - policy aimed at reducing data leaks (detection of unusual transmission directions),
   - blocking of communication with suspicious and risky URLs (URL filtering),
   - defining policies and rights to transfer files to known and controlled channels (elimination of attempts to transferring data secretly)

Figure 5 shows the implementation of resource protection.

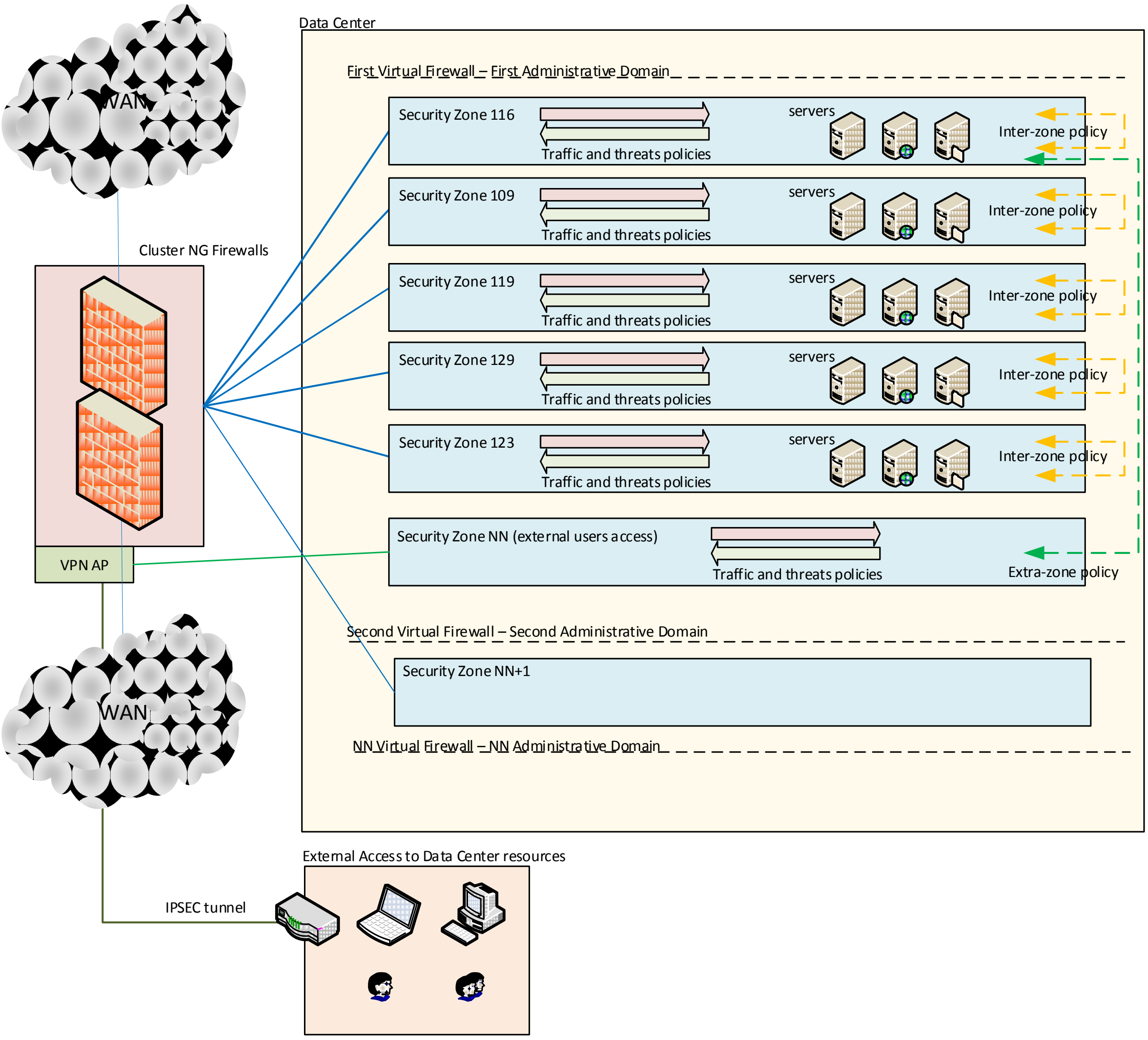
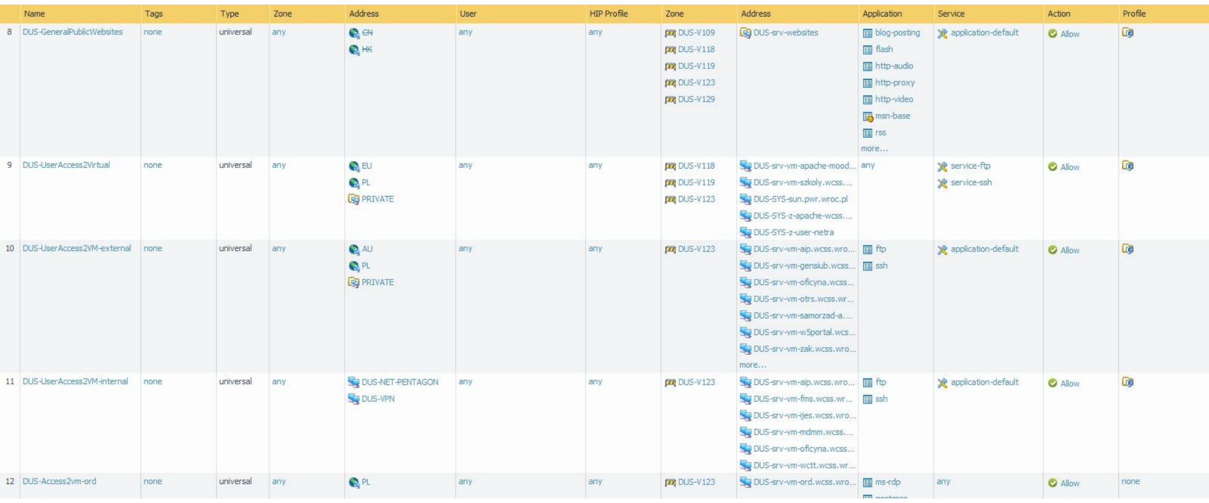

WAN
Cluster NG Firewalls
VPN AP
WAN
IPSEC tunnel
Data Center
First Virtual Firewall – First Administrative Domain
Security Zone 116
Traffic and threats policies
servers
Inter-zone policy
Security Zone 109
Traffic and threats policies
servers
Inter-zone policy
Security Zone 119
Traffic and threats policies
servers
Inter-zone policy
Security Zone 129
Traffic and threats policies
servers
Inter-zone policy
Security Zone 123
Traffic and threats policies
servers
Inter-zone policy
Security Zone NN (external users access)
Traffic and threats policies
Extra-zone policy
Second Virtual Firewall – Second Administrative Domain
Security Zone NN+1
NN Virtual Firewall – NN Administrative Domain
External Access to Data Center resources

Figure 5a. Implementation of the application firewall in the WCNS Data Center



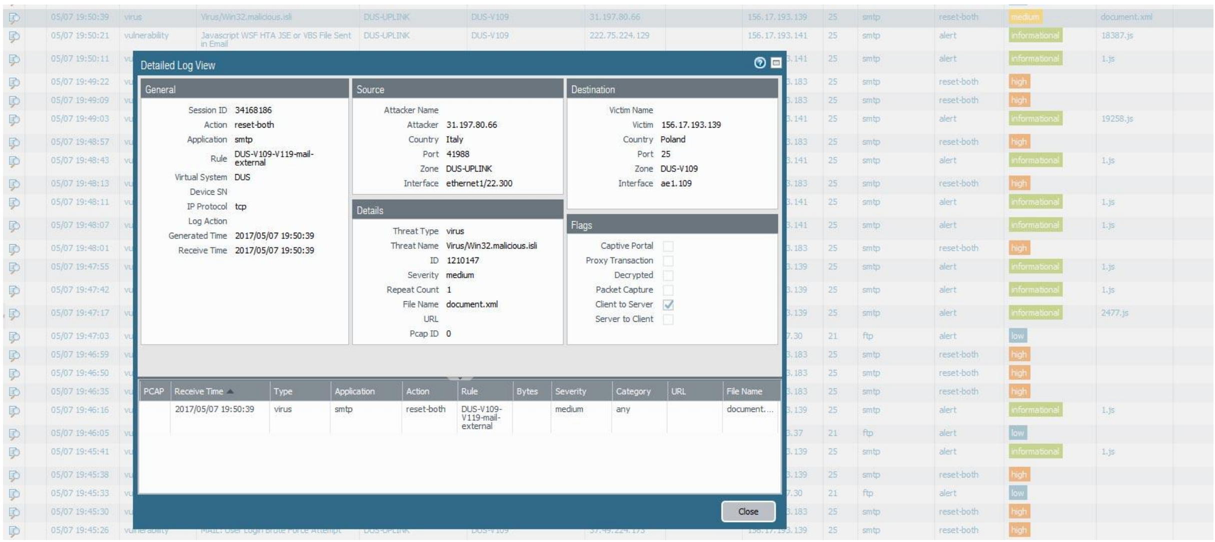
	Name	Tags	Type	Zone	Address	User	HIP Profile	Zone	Address	Application	Service	Action	Profile
8	DUS-GeneralPublicWebsites	none	universal	any	~~CN~~ ~~HK~~	any	any	DUS-V109 DUS-V118 DUS-V119 DUS-V123 DUS-V129	DUS-srv-websites	blog-posting flash http-audio http-proxy http-video msn-base rss more...	application-default	✓ Allow	
9	DUS-UserAccess2Virtual	none	universal	any	EU PL PRIVATE	any	any	DUS-V118 DUS-V119 DUS-V123	DUS-srv-vm-apache-mood... DUS-srv-vm-szkoly.wcss.... DUS-SYS-sun.pwr.wroc.pl DUS-SYS-z-apache-wcss.... DUS-SYS-z-user-netra	any	service-ftp service-ssh	✓ Allow	
10	DUS-UserAccess2VM-external	none	universal	any	AU PL PRIVATE	any	any	DUS-V123	DUS-srv-vm-aip.wcss.wro... DUS-srv-vm-gensiub.wcss... DUS-srv-vm-oficyna.wcss... DUS-srv-vm-otrs.wcss.wr... DUS-srv-vm-samorzad-a.... DUS-srv-vm-w5portal.wcs... DUS-srv-vm-zak.wcss.wro... more...	ftp ssh	application-default	✓ Allow	
11	DUS-UserAccess2VM-internal	none	universal	any	DUS-NET-PENTAGON DUS-VPN	any	any	DUS-V123	DUS-srv-vm-aip.wcss.wro... DUS-srv-vm-fms.wcss.wr... DUS-srv-vm-ijes.wcss.wro... DUS-srv-vm-mdmm.wcss.... DUS-srv-vm-oficyna.wcss... DUS-srv-vm-wctt.wcss.wr...	ftp ssh	application-default	✓ Allow	
12	DUS-Access2vm-ord	none	universal	any	PL	any	any	DUS-V123	DUS-srv-vm-ord.wcss.wro...	ms-rdp	any	✓ Allow	none

Figure 5b. Implementation of the application firewall in the WCNS Data Center

5.3 Results

Implementing the WCNS Data Protection System has made it possible to constantly detect numerous attacks on the IT infrastructure. Security administrators have acquired a tool for continuous threat monitoring throughout the unit. This solution integrated the tools and techniques used so far and allowed proactive actions (most of the actions were reactive and preventive).

Figures 6 illustrates sample security results (attack detection, password cracking attempts).



Detailed Log View

General

Session ID	34168186
Action	reset-both
Application	smtp
Rule	DUS-V109-V119-mail-external
Virtual System	DUS
Device SN	
IP Protocol	tcp
Log Action	
Generated Time	2017/05/07 19:50:39
Receive Time	2017/05/07 19:50:39

Source

Attacker Name	
Attacker	31.197.80.66
Country	Italy
Port	41988
Zone	DUS-UPLINK
Interface	ethernet1/22.300

Destination

Victim Name	
Victim	156.17.193.139
Country	Poland
Port	25
Zone	DUS-V109
Interface	ae1.109

Details

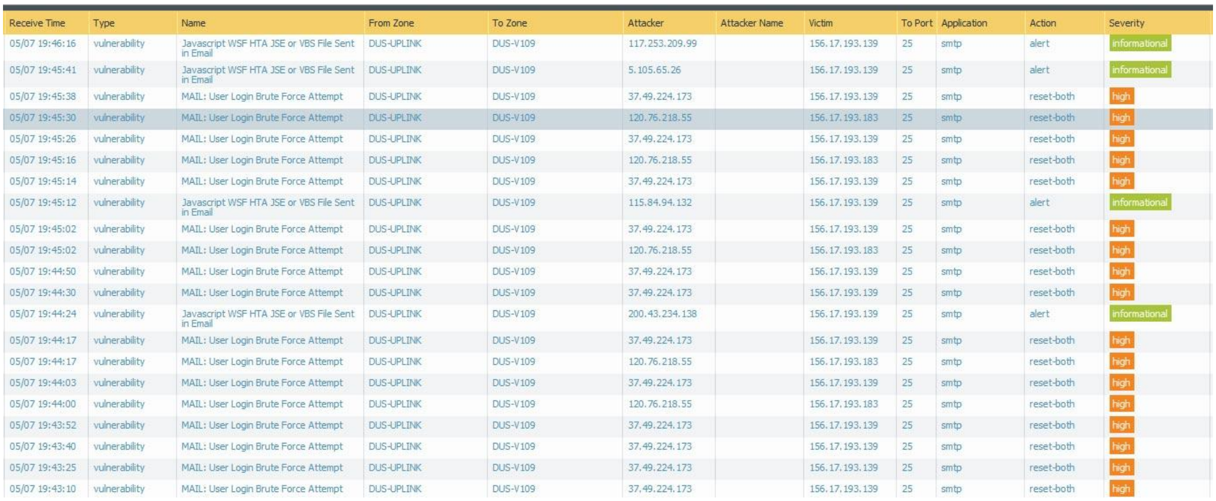
Threat Type	virus
Threat Name	Virus/Win32.malicious.isli
ID	1210147
Severity	medium
Repeat Count	1
File Name	document.xml
URL	
Pcap ID	0

Flags

Captive Portal	☐
Proxy Transaction	☐
Decrypted	☐
Packet Capture	☐
Client to Server	☑
Server to Client	☐

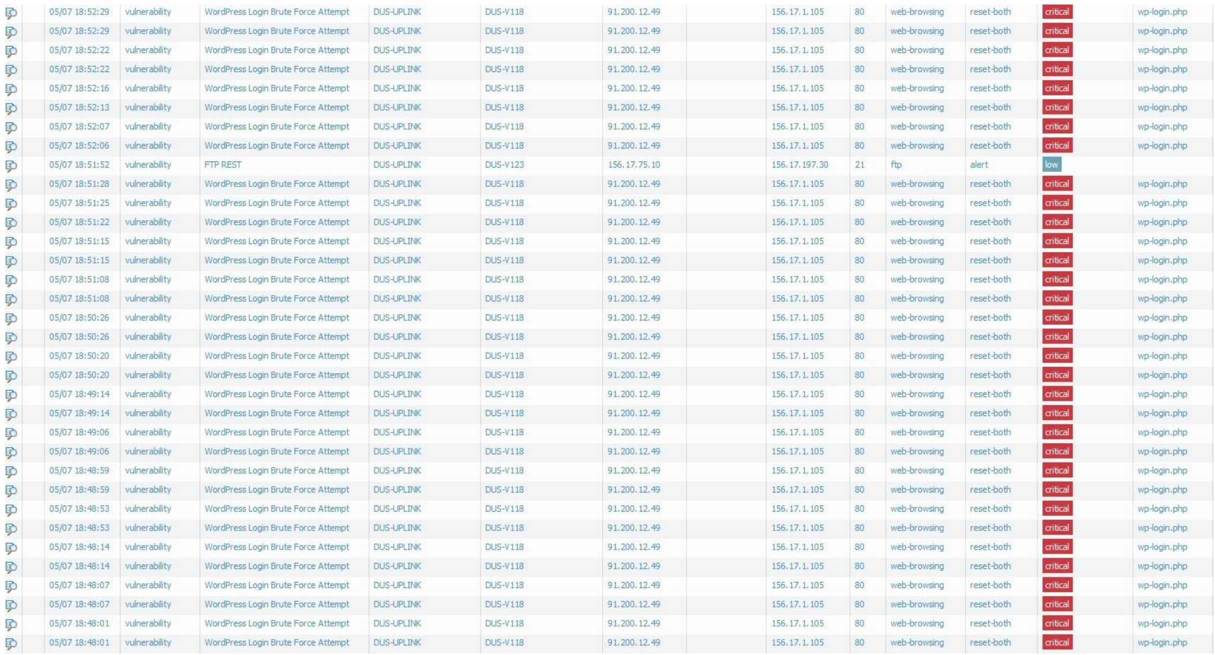
PCAP	Receive Time	Type	Application	Action	Rule	Bytes	Severity	Category	URL	File Name
	2017/05/07 19:50:39	virus	smtp	reset-both	DUS-V109-V119-mail-external		medium	any		document....

Figure 6a. Example of protection from threats - detection of mail virus



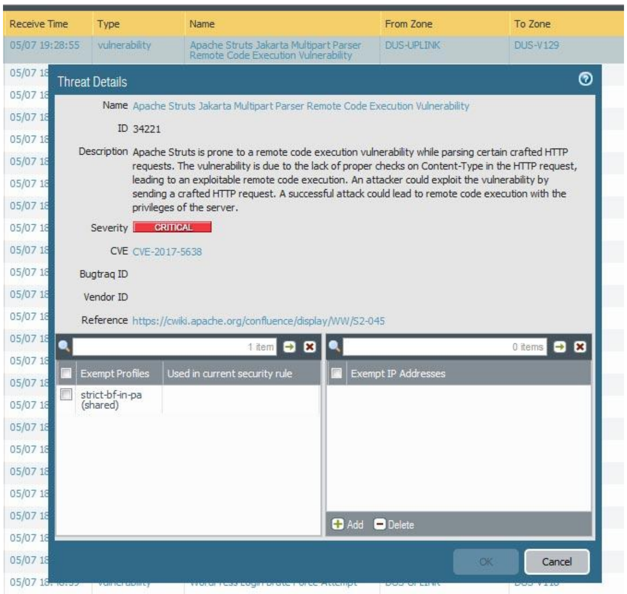
Receive Time	Type	Name	From Zone	To Zone	Attacker	Attacker Name	Victim	To Port	Application	Action	Severity
05/07 19:46:16	vulnerability	Javascript WSF HTA JSE or VBS File Sent in Email	DUS-UPLINK	DUS-V109	117.253.209.99		156.17.193.139	25	smtp	alert	informational
05/07 19:45:41	vulnerability	Javascript WSF HTA JSE or VBS File Sent in Email	DUS-UPLINK	DUS-V109	5.105.65.26		156.17.193.139	25	smtp	alert	informational
05/07 19:45:38	vulnerability	MAIL: User Login Brute Force Attempt	DUS-UPLINK	DUS-V109	37.49.224.173		156.17.193.139	25	smtp	reset-both	high
05/07 19:45:30	vulnerability	MAIL: User Login Brute Force Attempt	DUS-UPLINK	DUS-V109	120.76.218.55		156.17.193.183	25	smtp	reset-both	high
05/07 19:45:26	vulnerability	MAIL: User Login Brute Force Attempt	DUS-UPLINK	DUS-V109	37.49.224.173		156.17.193.139	25	smtp	reset-both	high
05/07 19:45:16	vulnerability	MAIL: User Login Brute Force Attempt	DUS-UPLINK	DUS-V109	120.76.218.55		156.17.193.183	25	smtp	reset-both	high
05/07 19:45:14	vulnerability	MAIL: User Login Brute Force Attempt	DUS-UPLINK	DUS-V109	37.49.224.173		156.17.193.139	25	smtp	reset-both	high
05/07 19:45:12	vulnerability	Javascript WSF HTA JSE or VBS File Sent in Email	DUS-UPLINK	DUS-V109	115.84.94.132		156.17.193.139	25	smtp	alert	informational
05/07 19:45:02	vulnerability	MAIL: User Login Brute Force Attempt	DUS-UPLINK	DUS-V109	37.49.224.173		156.17.193.139	25	smtp	reset-both	high
05/07 19:45:02	vulnerability	MAIL: User Login Brute Force Attempt	DUS-UPLINK	DUS-V109	120.76.218.55		156.17.193.183	25	smtp	reset-both	high
05/07 19:44:50	vulnerability	MAIL: User Login Brute Force Attempt	DUS-UPLINK	DUS-V109	37.49.224.173		156.17.193.139	25	smtp	reset-both	high
05/07 19:44:30	vulnerability	MAIL: User Login Brute Force Attempt	DUS-UPLINK	DUS-V109	37.49.224.173		156.17.193.139	25	smtp	reset-both	high
05/07 19:44:24	vulnerability	Javascript WSF HTA JSE or VBS File Sent in Email	DUS-UPLINK	DUS-V109	200.43.234.138		156.17.193.139	25	smtp	alert	informational
05/07 19:44:17	vulnerability	MAIL: User Login Brute Force Attempt	DUS-UPLINK	DUS-V109	37.49.224.173		156.17.193.139	25	smtp	reset-both	high
05/07 19:44:17	vulnerability	MAIL: User Login Brute Force Attempt	DUS-UPLINK	DUS-V109	120.76.218.55		156.17.193.183	25	smtp	reset-both	high
05/07 19:44:03	vulnerability	MAIL: User Login Brute Force Attempt	DUS-UPLINK	DUS-V109	37.49.224.173		156.17.193.139	25	smtp	reset-both	high
05/07 19:44:00	vulnerability	MAIL: User Login Brute Force Attempt	DUS-UPLINK	DUS-V109	120.76.218.55		156.17.193.183	25	smtp	reset-both	high
05/07 19:43:52	vulnerability	MAIL: User Login Brute Force Attempt	DUS-UPLINK	DUS-V109	37.49.224.173		156.17.193.139	25	smtp	reset-both	high
05/07 19:43:40	vulnerability	MAIL: User Login Brute Force Attempt	DUS-UPLINK	DUS-V109	37.49.224.173		156.17.193.139	25	smtp	reset-both	high
05/07 19:43:25	vulnerability	MAIL: User Login Brute Force Attempt	DUS-UPLINK	DUS-V109	37.49.224.173		156.17.193.139	25	smtp	reset-both	high
05/07 19:43:10	vulnerability	MAIL: User Login Brute Force Attempt	DUS-UPLINK	DUS-V109	37.49.224.173		156.17.193.139	25	smtp	reset-both	high

Figure 6b. Example of protection from threats - detection of mail password brute force attempt



05/07 18:52:29	vulnerability	WordPress Login Brute Force Attempt	DUS-UPLINK	DUS-V118	91.200.12.49		156.17.1.105	80	web-browsing	reset-both	critical	wp-login.php
05/07 18:52:29	vulnerability	WordPress Login Brute Force Attempt	DUS-UPLINK	DUS-V118	91.200.12.49		156.17.1.105	80	web-browsing	reset-both	critical	wp-login.php
05/07 18:52:22	vulnerability	WordPress Login Brute Force Attempt	DUS-UPLINK	DUS-V118	91.200.12.49		156.17.1.105	80	web-browsing	reset-both	critical	wp-login.php
05/07 18:52:22	vulnerability	WordPress Login Brute Force Attempt	DUS-UPLINK	DUS-V118	91.200.12.49		156.17.1.105	80	web-browsing	reset-both	critical	wp-login.php
05/07 18:52:16	vulnerability	WordPress Login Brute Force Attempt	DUS-UPLINK	DUS-V118	91.200.12.49		156.17.1.105	80	web-browsing	reset-both	critical	wp-login.php
05/07 18:52:13	vulnerability	WordPress Login Brute Force Attempt	DUS-UPLINK	DUS-V118	91.200.12.49		156.17.1.105	80	web-browsing	reset-both	critical	wp-login.php
05/07 18:52:07	vulnerability	WordPress Login Brute Force Attempt	DUS-UPLINK	DUS-V118	91.200.12.49		156.17.1.105	80	web-browsing	reset-both	critical	wp-login.php
05/07 18:52:06	vulnerability	WordPress Login Brute Force Attempt	DUS-UPLINK	DUS-V118	91.200.12.49		156.17.1.105	80	web-browsing	reset-both	critical	wp-login.php
05/07 18:51:52	vulnerability	FTP REST	DUS-UPLINK	DUS-V123	156.17.75.10		156.17.197.30	21	ftp	alert	low	
05/07 18:51:28	vulnerability	WordPress Login Brute Force Attempt	DUS-UPLINK	DUS-V118	91.200.12.49		156.17.1.105	80	web-browsing	reset-both	critical	wp-login.php
05/07 18:51:25	vulnerability	WordPress Login Brute Force Attempt	DUS-UPLINK	DUS-V118	91.200.12.49		156.17.1.105	80	web-browsing	reset-both	critical	wp-login.php
05/07 18:51:22	vulnerability	WordPress Login Brute Force Attempt	DUS-UPLINK	DUS-V118	91.200.12.49		156.17.1.105	80	web-browsing	reset-both	critical	wp-login.php
05/07 18:51:15	vulnerability	WordPress Login Brute Force Attempt	DUS-UPLINK	DUS-V118	91.200.12.49		156.17.1.105	80	web-browsing	reset-both	critical	wp-login.php
05/07 18:51:15	vulnerability	WordPress Login Brute Force Attempt	DUS-UPLINK	DUS-V118	91.200.12.49		156.17.1.105	80	web-browsing	reset-both	critical	wp-login.php
05/07 18:51:08	vulnerability	WordPress Login Brute Force Attempt	DUS-UPLINK	DUS-V118	91.200.12.49		156.17.1.105	80	web-browsing	reset-both	critical	wp-login.php
05/07 18:51:08	vulnerability	WordPress Login Brute Force Attempt	DUS-UPLINK	DUS-V118	91.200.12.49		156.17.1.105	80	web-browsing	reset-both	critical	wp-login.php
05/07 18:50:26	vulnerability	WordPress Login Brute Force Attempt	DUS-UPLINK	DUS-V118	91.200.12.49		156.17.1.105	80	web-browsing	reset-both	critical	wp-login.php
05/07 18:50:26	vulnerability	WordPress Login Brute Force Attempt	DUS-UPLINK	DUS-V118	91.200.12.49		156.17.1.105	80	web-browsing	reset-both	critical	wp-login.php
05/07 18:50:20	vulnerability	WordPress Login Brute Force Attempt	DUS-UPLINK	DUS-V118	91.200.12.49		156.17.1.105	80	web-browsing	reset-both	critical	wp-login.php
05/07 18:50:20	vulnerability	WordPress Login Brute Force Attempt	DUS-UPLINK	DUS-V118	91.200.12.49		156.17.1.105	80	web-browsing	reset-both	critical	wp-login.php
05/07 18:49:14	vulnerability	WordPress Login Brute Force Attempt	DUS-UPLINK	DUS-V118	91.200.12.49		156.17.1.105	80	web-browsing	reset-both	critical	wp-login.php
05/07 18:49:14	vulnerability	WordPress Login Brute Force Attempt	DUS-UPLINK	DUS-V118	91.200.12.49		156.17.1.105	80	web-browsing	reset-both	critical	wp-login.php
05/07 18:49:06	vulnerability	WordPress Login Brute Force Attempt	DUS-UPLINK	DUS-V118	91.200.12.49		156.17.1.105	80	web-browsing	reset-both	critical	wp-login.php
05/07 18:49:06	vulnerability	WordPress Login Brute Force Attempt	DUS-UPLINK	DUS-V118	91.200.12.49		156.17.1.105	80	web-browsing	reset-both	critical	wp-login.php
05/07 18:48:59	vulnerability	WordPress Login Brute Force Attempt	DUS-UPLINK	DUS-V118	91.200.12.49		156.17.1.105	80	web-browsing	reset-both	critical	wp-login.php
05/07 18:48:59	vulnerability	WordPress Login Brute Force Attempt	DUS-UPLINK	DUS-V118	91.200.12.49		156.17.1.105	80	web-browsing	reset-both	critical	wp-login.php
05/07 18:48:53	vulnerability	WordPress Login Brute Force Attempt	DUS-UPLINK	DUS-V118	91.200.12.49		156.17.1.105	80	web-browsing	reset-both	critical	wp-login.php
05/07 18:48:53	vulnerability	WordPress Login Brute Force Attempt	DUS-UPLINK	DUS-V118	91.200.12.49		156.17.1.105	80	web-browsing	reset-both	critical	wp-login.php
05/07 18:48:14	vulnerability	WordPress Login Brute Force Attempt	DUS-UPLINK	DUS-V118	91.200.12.49		156.17.1.105	80	web-browsing	reset-both	critical	wp-login.php
05/07 18:48:14	vulnerability	WordPress Login Brute Force Attempt	DUS-UPLINK	DUS-V118	91.200.12.49		156.17.1.105	80	web-browsing	reset-both	critical	wp-login.php
05/07 18:48:07	vulnerability	WordPress Login Brute Force Attempt	DUS-UPLINK	DUS-V118	91.200.12.49		156.17.1.105	80	web-browsing	reset-both	critical	wp-login.php
05/07 18:48:07	vulnerability	WordPress Login Brute Force Attempt	DUS-UPLINK	DUS-V118	91.200.12.49		156.17.1.105	80	web-browsing	reset-both	critical	wp-login.php
05/07 18:48:01	vulnerability	WordPress Login Brute Force Attempt	DUS-UPLINK	DUS-V118	91.200.12.49		156.17.1.105	80	web-browsing	reset-both	critical	wp-login.php
05/07 18:48:01	vulnerability	WordPress Login Brute Force Attempt	DUS-UPLINK	DUS-V118	91.200.12.49		156.17.1.105	80	web-browsing	reset-both	critical	wp-login.php

Figure 6c. Example of protection from threats - detection of WordPress password brute force attempt



Receive Time	Type	Name	From Zone	To Zone
05/07 19:28:55	vulnerability	Apache Struts Jakarta Multipart Parser Remote Code Execution Vulnerability	DUS-UPLINK	DUS-V129

Threat Details

Name: Apache Struts Jakarta Multipart Parser Remote Code Execution Vulnerability

ID: 34221

Description: Apache Struts is prone to a remote code execution vulnerability while parsing certain crafted HTTP requests. The vulnerability is due to the lack of proper checks on Content-Type in the HTTP request, leading to an exploitable remote code execution. An attacker could exploit the vulnerability by sending a crafted HTTP request. A successful attack could lead to remote code execution with the privileges of the server.

Severity: CRITICAL

CVE: CVE-2017-5638

Bugtraq ID:

Vendor ID:

Reference: https://cwiki.apache.org/confluence/display/WW/S2-045

□	Exempt Profiles	Used in current security rule
□	strict-bf-in-pa (shared)	

□	Exempt IP Addresses

Figure 6d. Example of protection from threats - detection of Apache Struts RCE

In recent years, across cyberspace, the number of attacks and their complexity have increased exponentially. This trend is also being observed in WCNS. Currently, it cannot be said that thanks to the implemented system, the number of attacks has been reduced. This number is constantly increasing. But we are now aware of the scale of threats and see how many attacks have been stopped. Certainly the detection and blocking of attacks has increased significantly.

6. Conclusions

To be able to prepare for defense against attacks, an integrated cyber protection system must be implemented. In order to do this properly and above all effectively, apart from buying a technical solution, one should approach the construction of cyber security as a continuous process. It is necessary to use all available knowledge, tools and organizational solutions. During design of the solution, attention should be paid to several important elements:

1. Knowing the organization's information and technology resources (classification, value for the company, and intruder).
2. Modeling threats.
3. Influencing the architecture of IT and organizational solutions in the organization.
4. Collecting event information to the central point.
5. Using tools for deep event analysis.
6. Using a preventive solutions (increases effectiveness).
7. Creating a dedicated team to monitor and respond to incidents.
8. Implementing a process to remove known vulnerabilities (change management and updates).
9. Sharing the acquired knowledge (including the use of Thread Intelligence)
10. Extracting conclusions from security incidents.

Various types of security incidents will occur more and more often. Every organization (public administration, small businesses, large corporations, or industries) is a potential victim of a computer attack. The use of any method of prevention is extremely important and in a significant number of attacks effective. Prevention, however, is always one step behind the attacker, and on the prevention itself you cannot really rely on cybernetic security.

If the prevention fails, it will be necessary to detect and neutralize the computer attack. It is good to be prepared for computer attacks, learn the tactics of the aggressors, build knowledge and exchange information. One cannot forget that cyber security is not a state, but it is a process. In response to cyber security in an organization, you need to be aware that an attacker can make many attempts and can make many mistakes. On the other hand, the cyber-security team cannot go wrong even once, because the consequences of the mistake of "blue team" are always expensive.

Intelligence-driven computer network defense is a necessity in light of advanced persistent threats. As conventional, vulnerability-focused processes are insufficient, understanding the threat itself, its intent, capability, doctrine, and patterns of operation is required to establish resilience. The intrusion kill chain provides a structure to analyze intrusions, extract indicators and drive defensive courses of actions. Furthermore, this model prioritizes investment for capability gaps, and serves as a framework to measure the effectiveness of the defenders' actions.

7. References

Hutchins, E. M., Cloppert, M. J., Amin, R. M., 2011. Intelligence-driven computer network defense informed by analysis of adversary campaigns and intrusion kill chains. Leading Issues in Information Warfare & Security Research, 1, 80.

Cichonski, P., Millar, T., Grance, T., Scarfone, K., 2012. Computer Security Incident Handling Guide, National Institute of Standards and Technology. Special Publication 800-61 revision 2, March 2008.

Roberts, S. J., Brown , R., 2017. Intelligence-Driven Incident Response, Outwitting the Adversary, O'Reilly Media, 2017

Yadav, T., Rao, A. M., 2015. Technical Aspects of Cyber Kill Chain. In International Symposium on Security in Computing and Communication (pp. 438-452). Springer International Publishing.

MacGregor R., 2015. Diamonds or chains - Cyber security updates, < http://pwc.blogs.com/cyber_security _updates /2015/05/ diamonds-or-chains.html > [Accessed 1 May 2017]

Vitae

Ireneusz Tarnowski is a Senior Specialist in Wrocław Centre for Networking and Supercomputing, where he deals with the administration and security of network services. Graduate from Computer and Cyber Security Management. In the field of IT systems security he effectively combines the gained knowledge with over 11 years of experience. Being an independent consultant he analyzed hundreds of computer incidents. Engaging in the development of methods for detection and analysis of threats to widely understood IT infrastructure, he prepares technical and organizational solutions aimed at increasing the security level of the organization. Member of Information Security WCNS Team, the PIONIER CERT and ISACA.