Approaching a DoS attack using change and risk management methods

Stefan Pavlov[1], Vesna Dimitrova[2], Ljupcho Antovski[3]
Faculty of Computer Science and Engineering
Ss. Cyril and Methodius University, Skopje, R.N. Macedonia[1,2,3]
stefan.pavlov47@gmail.com, vesna.dimitrova@finki.ukim.mk, ljupcho.antovski@finki.ukim.mk

Abstract: *The Information Technology security threats are emerging with each day passing by. The implementation of the technology into every field of society brings changes. Finding a way to manage these changes would be a success, and, by doing so, it would mitigate the risks they bring. Data transmission nowadays is unsecure like never before. Challenging is the way that should be found to cope with these kinds of evolutionary changes. Among the top threats in networks lies the DoS attack. It has been a long time since this kind of attack is around, but that doesn't reduce the fact that this type of attacks is still dangerous and devastating. In order to cope with this kind of attack, we need to know how to manage risks and changes during a DoS attack. Because of this, it is very important that defensive mechanisms are implemented and integrated so that unauthorized access would be prevented from accessing your network or data. This refers to individuals and everyone else working in companies that are working in the field of IT, because at some point, we all share the same thing-devices (mobile phones, personal computers, devices at work, etc.). The base of the IT foundation is knowing how to protect yourself and your data. Due to this, we need to work hard and exploit every possible threat and attack from the inside out. Not only to reduce or mitigate the already occurred impact, but also to prevent these types of failures from happening in the future.*
Keywords*: CHANGE, RISK, SECURITY, DATA*

1. Introduction

It is certain that when dealing with Information Technology (IT), changes will occur. In order to make progress in this area of technology, you have to be able to make the right decisions at the right time, and by doing so, you will be effective. As it is said in [1], if you want to be able to act efficiently and make wise decisions, most of your IT personnel must assess the risks involved in making the change. By the comprehension of the risks, the project manager can be at ease when dealing with changes on entire projects. These changes may affect the project a lot, including the budget, quality, sources etc. The main source of risks today comes from the cyber area, or the main threats are the cyber threats.

This is why in this paper we discuss risk associated with late changes which are done to a network by a recent DoS attack. The paper itself covers the risk and the change management methods when dealing with a DoS attack. At the end of the paper, there is an example which can provide the reader with adequate opinions which can be useful while handling DoS attacks. By doing this, the already occurred damage from a DoS attack would be reduced to its minimum.

2. Change and Risk Management in IT

As the innovation of technology does not tire, it has brought new threats. In fact, the threats are emerging faster than they can be assessed. This refers to the whole world of IT professionals. This technology may have made our lives easier, but it is met by similar innovation technologies which could take advantage of cyber systems for other gains. It is possible that the threats are sponsored by nation-states and the defense systems against those kinds of threats are failing.

While facing these types of threats, we need to provide ourselves with the best defensive mechanisms, which are provided by the change and risk management methods in order to prevent such attacks from happening.

These are modern times, and in modern times with modern technology, come modern network threats. About these threats you can read below.

In [2], a modern network threat paper that has been done recently, ranks the top fifteen threats. If we go back in 2018, the threats that were causing the most network security issues were: Malware, Web-Based Attacks, Phishing, Denial of Service (DoS), Spam, Botnets, Data Breaches, Insider Threat, Physical Manipulation/Damage/Theft/Loss, Information Leakage, Identity Theft, Cryptojacking, Ransomware and Crypto Espionage.

According to [2], among the top fifteen, as mentioned above, are the DoS attacks which are slowly but surely, emerging. More and more DoS attacks occur every day, and this is why, we need to find a way to cope with these types of attacks. In order to understand the attack, we need to know how to analyze and understand the threat first.

As we move on further in [2], there is a classification done on DoS attacks. This classification is based on the idea that if we are willing to deal with the threat, it is essential to understand the source of it. Just as it is said [2], we can see that there are two types of issues regarding this topic and those can be noted as threat agents and attack vectors. As pointed out before, threat sources consist of two entities:

Threat Agents

By [2], the threat agents are the actors, individuals or organizations, who are able to generate or create a threat. The main concern of these agents is their identity. That is why they try to mask it and they claim identification with another group. They usually do this by posting such materials in fake news and social media.

Attack Vectors

Regarding the attack vectors, they are the path by which a threat agent can gain access to a computer or network for the purpose of malicious activity. The table below is as well from the paper mentioned above or [2].

We can see that the DoS attacks to networks are numerous and potentially devastating. Regarding [3], we as well think that many types of DoS attacks are well known and the bigger part of them are quite effective to stop the communication in the networks. This is because this kind of attacks include the use of single computer or multiple computers, called zombies. This is a technique known as simple DoS attack and later on as Distributed Denial of Service (DDoS) attack.

The following part involves a brief description of DoS attacks in order to better comprehend the rest of the paper. If we try to define it, then a DoS attack would be an attack which is launched to make networks and systems' resources unavailable for the legitimate users.

In [3], it is said that most of the hackers have three things in mind. The first one is to find a way through which they can get the secret information. And this would be the way to compromise the confidentiality. The second one involves gaining access to the confidential information to change or modify it. This means the compromising of integrity. The third one is done to compromise the availability. Many of the DoS attacks are made by exploiting the

weaknesses in TCP/IP stack protocols. The classical examples of those DoS attacks are TCP Syn Flood, UDP Flood, ICMP Flood, Smurf and Incomplete HTTP Requests, etc.

Table 1: *Annual change in raking of the top fifteen threats according to the Evolution Threat Landscape (ETL)* [2]

Top Threats	Year						
	2018	2017	2016	2015	2014	2013	2012
Malware	1	1	1	1	1	2	2
Web-Based Attacks	2	2	2	2	2	1	1
Web Application Attacks	3	3	3	3	3	3	3
Phishing	4	4	6	8	7	9	7
Denial of Service	5	6	4	5	5	8	6
Spam	6	5	7	9	6	10	10
Botnets	7	8	5	4	4	5	5
Data Breaches	8	11	12	11	9	12	8
Insider Threat	9	9	9	7	11	14	-
Physical Manipulation/Damage/Theft/Loss	10	10	10	6	10	6	12
Information Leakage	11	13	14	13	12	13	14
Identity Theft	12	12	13	12	13	7	13
Cryptojacking	13	-	-	-	-	-	-
Ransomware	14	7	8	14	15	11	9
Cyber Espionage	15	15	15	15	14	-	-
Exploit Kits	-	14	11	10	8	4	4

A) Classification of DoS Attacks

The Table II, which is from paper [3], shows the classification of DoS/DDoS attacks.

Table 2: *Classification of DoS attacks [3]*

DoS/DDoS	
IPv4	IPv6
Layer 4 (Transport layer) Attacks	Layer 4 (Transport layer) Attacks
Layer 7 (Application layer) Attacks	Layer 7 (Application layer) Attacks
-	Neighbor Discovery Protocol Attacks

B) Layer 4 Attacks

Wireless TCP-Flood Attack

When a client tries to make a connection with a server, both machines, the clients' and the server, exchange a set of messages sequentially. This is known as Three Way Handshaking. As it is described in [3], first, the client sends a SYN (synchronization) message to the server. The server then sends back a SYN-ACK (acknowledgment) message to acknowledge the SYN message send by the client. Finally, the client then responds with an ACK message to finish the establishment of the connection. At last, the connection is then opened and as a result, data exchange between the server and the client start taking place. To exploit this, the one who attacks, sends a series of SYN messages to the user, or the victim, and as a result, the victim responds back with a SYN-ACK message and then it waits for some time for an ACK to come back to finish the connection establishment. Due to the fact that the attacker has sent the SYN messages with spoofed source address, there will not be any ACK return due to absence of such addresses. And, as a final result, the several partially opened connections fill the queue and memory buffers, and due to that, users will not be able to get services any time soon.

UDP-Flood Attack

The UDP-Flood occurs when two services CHARGEN (character generator) and ECHO of UDP protocol generate a technique through which the flood can be launched. It happens so that the attacker targets and overwhelms random ports on the host.

ICMP(v6)-Flood Attack

ICMP (v6)-based utility ping (Packet Internet Groper) uses a technique known as echo response mechanism. When conducting this attack, the attacker sends large amount of packets to the victim with different spoofed invalid source IP addresses.

Smurf Attack

This type of attack is similar to the ICMP (v6) flood attack because it uses the echo response mechanism of ICMP (v6). It is mentioned in [3], that in this attack, the attacker does a broadcast of packets with spoofed source IP address targeted to the victim. Because the packets are received by all the nodes within the network, each and every node responds back. Then, the victim's machine gets large amount of echo responses, and it gets exhausted.

C) Layer 7 Attacks

Incomplete HTTP requests using GET method

If we pay attention to what is written in [3], then this attack is based on how the client sends the data to the web server while communication goes on between them. In this attack, the client sends HTTP requests to the web server but in a different way. After sending multiple incomplete requests, the client exhausts the server's resources. As a result, these requests consume all the available resources on the server, thereby denying the legitimate users' requests.

Incomplete HTTP requests using post method

By [3], this type of attack is almost the same as the Incomplete HTTP requests using GET method. The thing that is different here is that the client himself is the one who is sending the incomplete HTTP requests with the aid of POST method and not GET.

HTTP requests using HEAD method

As it is referred to in [3], this attack, or HEAD method differs from the GET method only because while using HEAD method, while the server is giving the response, it must not include a message body. But, if it does include a message body, the process itself will save resources on the attacker's side which helps the attacker find out which page is more expensive for the server.

3. Approaching a DoS attack using change and risk management methods

The nature of the denial of service attacks, as mentioned in [4], lies in making the resources unavailable to the victim. It can be described as an attempt by the attackers to try and stop legitimate users of a computer service from using it. However, as any sort of information issue connected to network security, the fight against denial of service is some type of a training in risk and change management. In order to reduce the risk to its minimum, you must

be able to make right decisions at the right time, as well as technical decisions at critical times.

If we want to cope with the risks posed by denial of service, we would need a multi-pronged approach, recommended in [4]. This includes:

A) Make your business as robust as you possibly can so it can survive all the threats and attacks. This means that your business should be able to adapt and survive at all costs.
B) You need to commit yourself and your team on designing a line of defensive mechanisms, which will ensure that the services will continue to work despite an eventual attack or a failure.
C) In most countries people say that good things happen to good people, but that cannot refer to the "netizens". With other words, if you are a good netizen, it does not mean that you will not get attacked or your system will not fail. So, you need to brace yourself because the threat done to your network is proportional to the extent that a lot of attacks might follow in the future.

When speaking about this sort of network threat, we need to consider the finance or the money factor. This means that every lousy job may cost you a lot of finances, and on the other hand every well spent finances may get you more users and more profit.

If we look at some DoS attacks one time, we cannot see the clear picture. DoS attacks should be reviewed few times, then analyzed, and then you might get an idea of what the attack might be about. This means that there are hidden costs which are associated with this type of attack. For an example, as in [4], the direct target of DoS or DDoS attack may not be the only victim. So, the attack against one of the sites, can and might affect the network resources of several or all sites. This works the same with resources, when the resources you share with your parties are consumed, you will be left with no resources, and that is when you are left out with no service. If this happens to you, it means that you will have lag or increased network latency or packet loss, or it might even come to a full outage.

Fair amount of finances should be spent on the logging systems, because those are the systems that need to handle significant deviations when there is a big amount of data being logged during attacks.

It would be ideal, if logging systems used an out-of-band channel, just so that logging traffic would not add up to the DoS traffic and then passed to the network. If this comes to its culmination, then the next thing you know is having full mail queues and an incoming outage.

There are a lot of options to consider here, when referring to the defense mechanisms of a network system, since the source of the attack is always unknown. That is why we need to keep our systems up to date, and upgraded, in case anything happens. just so we and our data would be safe and sound.

4. Security spending example

Let's make a story worth telling here. You are an owner of a TV services provider, and its an IP TV company. You are located in Macedonia, and the budget to defend in this country against these types of attacks is $ 20,000. I know its not much, but if you were here, it would mean a lot for you due to the fact that an average salary in this country is $ 450 according to the Macedonian State Statistical Office. Just to be clear, this is your budget that should cover all your costs on staff, equipment etc. Going back to the story, in my opinion, this is how your organization should spend those funds:

Example 1

You will be obliged to excess the capacity just so you could absorb some attacks, then you must hire experienced staff, and at last, you must provide defensive network equipment. So this is how your expenditures should look like:

$4,000 extra bandwidth and router through put

$10,000 experienced, highly skilled staff

$6,000 firewall, load-balancing, traffic-shaping technology

This is not the only option though. You may consider changing anything in this illustration. According to [4], when deciding on your company's response to DoS attacks, consider these couple of questions: What are the chances of an attack hitting your company? What are the chances of an attack being of a certain type and/or magnitude? What level of risk is acceptable? How important is the Internet to your business? How long can you function without some or all Internet services? Which services you cannot function without?

Meaning that we would like to make a discussion out of these questions, it would probably turn out to be like the following.

Starting with the first one, or what are the possibilities of an attack on your company? The possibilities of getting a DoS attack vary on the popularity of your company. This means that if you are a low profit company or organization, you have nothing to worry about, or you probably will not be a target. On the other side, if you have lot of costumers and working personnel in your company it would mean that you have a lot of data stored in your base. Cracking that base would be a challenge for an attacker, because a lot of data leads to a lot of money.

Moving on to the second one, or what are the chances of the attack being a certain type or magnitude? This question can be answered similarly to the previous one. Basically, if you are a low-profile organization, the attack you might expect might cost few thousand dollars, and on the other hand, if you are a high-profile organization, the attack that penetrates your systems might cost you millions of dollars or even more.

The third one, or what is the level of risk that is acceptable? This is an issue regarding the staff on the top of the pile in the company. Those are the ones who should make the decisions and put the boundaries on which risks are and which risks are not acceptable. Of course, the answer of this question would be, any risk that can be mitigated, is acceptable.

The fourth one refers to the importance of the Internet to your business. As a thing that makes our lives easier with all the feeds and notifications on our screens that provide us with the information we need, one would say that the Internet has become a pretty important part of our lives.

Last but not least, how long can you function without Internet services? The answer of this question is simple. If your working position depends on Internet services, then you cannot function without them. However, if you can do your job while not being online and not needing any Internet services, then you can go back to the dark age and not bother with these things.

And the last one, what are the services you cannot function without? For me, personally, the wireless services are something that has changed everything in terms of technology. Everything you need or everything to want is on the palm on your hand – on your screen. Through our mobile devices and gadgets, we can do anything we want and the coolest thing is that we are not bonded by any wire or cable or any kind of physical transmission medium.

5. Conclusion

The purpose of this paper is to give the reader a work framework when facing a DoS attack while using change and risk management methods, which includes:

- Change and risk management in IT,
- Modern day network threats, and
- Approaching a DoS attack using change and risk management methods.

This work describes what you need to know when facing a DoS attack on any type of network. And by doing that, you will either prevent your network from getting attacked or mitigate the attack's impact that has already occurred.

Besides the change and risk management in IT, which provides us with essential information on how to cope with DoS attacks, in this work, you can find the most recent research done on DoS by Imperva Research Lab as well as an example on how you should spend a budged in order to have a safe and well protected network.

To conclude, the topics that this paper provides are the fundamental key elements in getting to know DoS attacks and security issues regarding them.

6. References

1. Byron J. Williams, Jeffrey Carver, Ray Vaughn, *Change Risk Assessment: Understanding Risks Involved in Changing Software Requirements*, (Department of Computer Science and Engineering, Mississippi State University, MS, USA, **2**, 2006).
2. Houssain Kettani, Polly Wainwright, *On the Top Threats to Cyber Systems*, (The Beacom College of Computer and Cyber Sciences, Dakota State University, S.Dak., USA; Department of Computing and Information Sciences, Valparaiso University, IN, USA, **2**-**4**, 2019).
3. Nikhil Tripathi, B.M. Mehtre, *DoS and DDoS Attacks: Impact, Analysis and Countermeasures, Institute for Development and Research in Banking Technology*, (Hyderabad, India, **2**-**5**, 2013).
4. Allen Householder, Art, Manion, Linda Pesante, George M. Weaver, *Managing the Threat of Denial-of-Service Attacks*, (Carnegie Mellon University, PA, USA, **1**-**4**, 2001).