Security Investments

Economics of Cyber Security, Assignment Block III

Xander Bouwman, Dereck Bridie, Paul van der Knaap, Gouri Calamur Viravalli, Daan van der Valk

Abstract *Distributed Denial-of-Service attacks by various actors pose a major threat to information availability. The study of DDoS detection, prevention and mitigation has gained importance with the rise in attack volume and sophistication. E-commerce websites are at risk, due to incurring loss when unavailable as a result of DDoS attacks. This paper identifies actors involved, and looks into effective security analysis and risk reduction strategies for DDoS attacks, and in particular, e-commerce website Zalando. This company's Annual Loss Expectancy is calculated using probabilistic values, and this is used to find Return on Security Investment (ROSI) for investing in services of cloud DDoS mitigation provider Cloudflare.*

1. Introduction

An attacker disrupts services of hosts connected to the internet by overloading the targeted system with requests, causing what is called a denial-of-service attack. Modern distributed DoS attacks (DDoS) are non-trivial to block, as incoming traffic originates from many sources and pluriform packets are crafted to resist filtering. When an attack consists of more than one type of DDoS, it is called a multi-vector DDoS attack. In this paper, we identify the actors involved in this security issue, and identify and analyze the risk strategies that the actors can adopt to tackle the issue at hand. We also calculate Return on Security Investment (ROSI) for the best risk strategy identified.

1.1 E-commerce and DDoS attacks

Many people prefer to shop from e-commerce websites today due to its easy of use and convenience. However, these online retailers often fall victim to DDoS attacks. E-commerce sites experience a lot of fluctuation in traffic, and influxes that coincide with new products, discount sales etc., hence making them very vulnerable to these attacks. If a company does not have proper DDoS protection, it is liable to loss. This risk will be further explored in the paper for the case of major e-commerce provider Zalando. Fortune 1000 companies lose up to a few billion dollars every year due to crashed websites caused by DDoS attacks and other unplanned outages [6].

1.2 DDoS Statistics

DDoS attacks in e-commerce websites have been ever increasing, since the online shopping trend caught on. Since 2015, the general trend is that the frequency of attacks is still growing [6,10]. The peak size of the attacks are also still growing, but for e-commerce in particular it seems that the peak size is lowering. However, the attacks are still a real threat, with attack size peaks between 1 and 5 Gbps in the last few quarters. But, 92% of such DDoS attacks can be mitigated with the help of DDoS protection services - the most common one being Cloudflare [5].

1.3 Problem Statement

This paper explores how to design the best risk reduction strategy for Zalando as the target of DDoS attacks, using the Return on Security Investment methodology.

2. Methodology

In order to identify strategies for threat reduction, the threat of DDoS attacks to and e-commerce company needs to be defined properly. First, the problem owner and threat actors involved are examined. Second, possible threat reduction strategies are evaluated. Third, data are gathered and assumptions are made about the costs and benefits for the chosen strategy. Based on this, the Return-on-security-investment for the chosen strategy is calculated [14].

2.1 Metrics and their use

The metric considered in order to evaluate the security goal of availability is service uptime [2], measured by minutes of downtime per year. The criterium for downtime is when latency is too high for Zalando's customers to use the service.

3. Recognizing problem owners

The problem owners of such an ecommerce website that faces DDoS attacks begins with the company owners. The stakeholders of the company, partners and other contributors also face monetary loss depending on their level of involvement. Zalando has about ten shareholders, and their ownership varies from 3% to 31%.

4. Recognizing actors

The *Cyber Security Assessment Netherlands* [8] by the National Cybersecurity center of the Netherlands lists threats in the form of actors that can be used in our case study.

4.1 Shop owner

We will use an online shop owner as the product owner in this case. A shop owner wants their commerce platform to stay online so that customers can purchase goods and so revenue can be generated. To simplify the calculations, we will assume that all of the revenue generated by the company comes from online sales exclusively.

4.2 Professional criminals

The goal of professional criminals is monetary gain. The way they can achieve this is by using digital attacks (ie, accessing the webshops funds) or using extortion tactics to force stakeholders to pay in exchange for withholding vital information.

The Cyber Security Assessment Netherlands (CSAN) also notes that professional criminals are becoming more purposeful in extortion and that the actions are becoming more impactful for victims, as more attacks use a form of digital extortion. An example of this are the attacks using WannaCry [7], a software tool which takes a victim's data hostage by encrypting their hard drive until the attacker gives them the decryption key. In exchange for money, the attacker will release the key to the victim.

In addition to the ransomware, the CSAN mentions the use of DDoS attacks and use downtime of servers to extort victims. The criminals can also try to breach a system to access customer's personal data and extort individuals with this information.

4.3 Terrorists

Although the role of terrorists might not be significant now, this may increase in the future, as the future trends towards the use of online shopping more and more, also for daily groceries. As the usage grows and becomes more common, a terrorist attack could have an increasingly larger effect on society's infrastructure. For example, if common online grocery stores become unaccessible while people depend on them, that could cause panic.

However, the CSAN document reports, the heavy use of digital attacks has not yet been seen; terrorist groups focus on keeping their communications encrypted and execute small-scale attacks that "require little capacity and few resources".

4.4 Cyber vandals and script kiddies

The CSAN document reports that the threat from cyber vandals and script kiddies is increasing because of the growing availability and accessibility of tools that are capable of executing online attacks. For example, "booter services" are readily available, a service that will execute a small sized DDoS attack for very low prices. The motivation for these attacks is to demonstrate their abilities or as a challenge or prank. The groups carrying out these attacks are often minors.

4.5 Cyber researchers

Though these researchers often do not cause monetary harm, it is often useful to mention because of bounty programs that still cost money. These bounty programs as well as responsible disclosure agreements help organisations improve security and develop solutions and controls. However, published research could still help malicious parties and damage companies.

4.6 Competitors

Competitors are another actor in this model. The motives could be, according to the CSAN report, affecting the confidentiality of systems for financial gain, improving their competitive position, and selling the victim company’s customer’s data.

5. Risk strategies

This section examine possible DDoS risk reduction strategies and evaluates their application to Zalando, concluding that cloud mitigation providers are most appropriate solution to reduce risk of a DDoS attack for most businesses, including Zalando. The elements of a ROSI for the chosen strategy are then developed, leading to an estimation of the ROSI for a risk reduction strategy using the Cloudflare cloud mitigation provider.

5.1 Risk reduction strategies for DDoS attacks

This paper assumes general preventative measures have already been taken, such as keeping systems up to date with the latest security patches [1]. These are not included as a strategy.

The first category of solutions makes use strategies to filter or deflect[1] malicious incoming traffic. This is hard for modern sophisticated attacks which make use of pluriform packets and IP-spoofing

[1]. High upfront investments in development hours or specialized on-site networking devices are required, which would remain inactive unless an attack takes place. Therefore we can already conclude that unless an organization is being attacked a significant portion of the time, such solutions will have a very low ROSI. In addition for our case, Zalando is geographically dispersed and would therefore need do these investments for each location from where it serves data. This is considered infeasible.

The second category of solutions consist of cloud DDoS mitigation providers, or resource multiplication [1]. On subscription basis these services offer load-balancing and as required a large amount of bandwidth to scale up. As such large bandwidth is only ocassionally needed, resources may be pooled at the cloud mitigation provider and costs are expected to be lower. Additionally ISPs offer such services, generally on smaller scale. Due to the scale of traffic and geographic dispersion of Zalando however, a large cloud provider will offer better fit to the services required.

Cloudflare is one of the largest DDoS protection services [11]. As Cloudflare is able to withstand all DDoS categories (in terms of bandwidth) [12], it offers an attractive control. Their enterprise plan includes real-time support and is offered for $5000/month. The DDoS risk reduction strategy will therefore consist of subscribing to the services of the provider Cloudflare. The elements of the ROSI of this strategy will now be developed.

5.2 Zalando operational gross profit

To estimate Zalando's losses as a consequence of DDoS attacks, we need to choose what costs and benefits to select for the assumed loss per minute downtime. To solely take the revenue into account, would be an oversimplification. When the webshops are offline, there are indeed no profits; however, the purchase of the related goods of this missed revenue vanishes. Therefore, we decided to subtract the cost of materials (part of the cost of sales), and the fulfillment cost (part of the selling and distribution costs). For 2016, we define the *operational gross profit*:

Revenue from the sale of merchandise [3]	3,553.1 million EUR
Cost of materials [3]	- 1,823.4 million EUR
Fulfillment costs [3]	- 847.8 million EUR
Operational gross profit	*881,9 million EUR*

This results in an average operational gross profit of 1673.31 EUR per minute.

Other costs, like administrative expenses, third-party services, infrastructure cost, and marketing costs, are not taken into account. Although those cost factors might be affected by a DDoS attack, there is no apparent linear relationship and should thus not be related to minutes of downtime directly. Although this is a simplification, we believe the operational gross profit reflects the most representative metric to the losses when experiencing downtime.

5.3 Annualized Loss Expectancy estimation

To compute the Return of Security Investment (ROSI), first the Annualized Loss Expectancy (ALE) is determined. Traditionally, this the *ALE* is computed as follows:

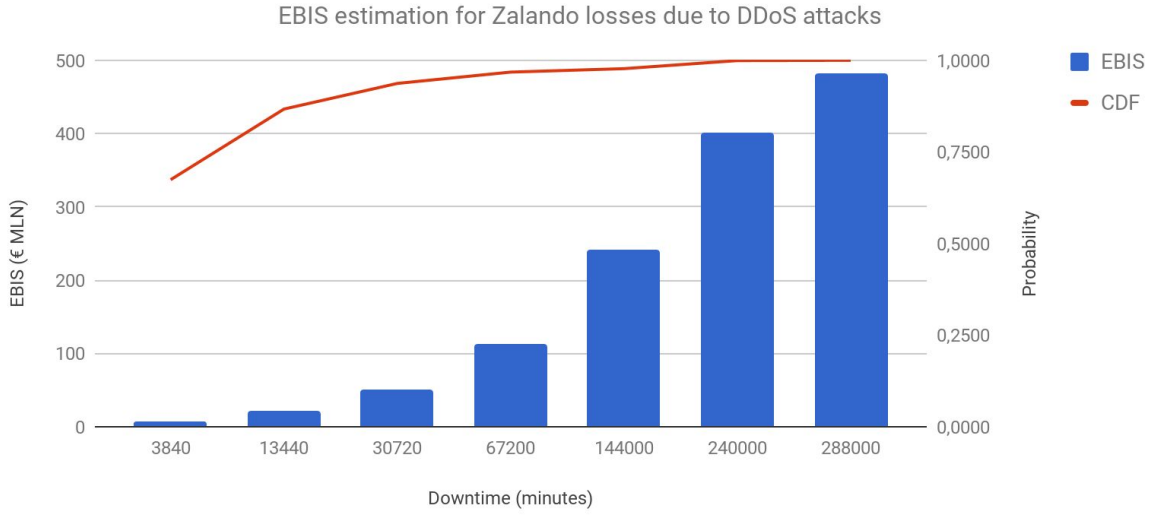
$$ALE = Annual\ rate\ of\ occurrence\ (ARO)\ \times Single\ Loss\ Expectancy\ (SLE)$$

However, the inputs of this simple formula cannot be described accurately with a single value. The annual rate of occurrence—number of DDoS attacks in a year—and the single loss expectancy is not easily determined, but rather estimated using probabilistic methods. The total downtime is assumed to be related linearly to the loss.

Organizations faces an average of 32 attacks per quarter [4], and the attack length is typically distributed as follows [7]:

Attack duration	2 hours	7 hours	16 hours	35 hours	75 hours	125 hours	150 hours
(in minutes)	*120*	*420*	*960*	*2100*	*4500*	*7500*	*9000*
Probability	0.6742	0.1928	0.0700	0.0309	0.0094	0.0220	0.0008

Multiplication of the expected downtime due to DDoS attacks with the operation gross profit during that time, yields the following result:



6. Calculating ROSI

In the most probable scenario, Zalando faces with 3840 minutes of downtime per year. If there are no controls in place at all, this results in a loss of 6.3 million EUR. As stated earlier, the Cloudflare enterprise solution costs $5000/month [13], resulting in € 51.140 of costs per year. As Cloudflare protects against all DDoS attacks that are likely to happen, we expect all risk to be mitigated. In the most probable scenario of 3840 minutes of downtime, the ROSI is computed as follows:

$$ROSI = \frac{ALE_0 - ALE_1 - solution\ cost}{solution\ cost} = \frac{6{,}425{,}510.40 - 0 - 51{,}140}{51{,}140} = 124.65 = 12465\%$$

This very high value indicates that it is a very good control for Zalando to implement as millions can be saved with an investment of only about fifty thousand euros. Therefore, it should be an obvious choice for them to invest this amount. Even if the enterprise plans would effectively cost ten times as much, or if the impact would be 10 times as much, the ROSI is still very high.

7. Conclusion

DDoS attacks can cause major monetary and reputational loss to both stakeholders and employees of the company, and their customers. The severity of a DDoS cannot be predicted and hence risk strategies for preventing them are essential. This paper concludes that the best risk strategy for the company Zalando is to protect itself from DDoS attacks by using a cloud based DDoS protection service, as it will provide a significant return based on the ROSI model.

Making use of the facts available on the number of DDoS attacks the company faces per quarter, this paper creates a probability distribution, and also calculates Annual Loss Expectancy based on these values. According to our research, the Return on Security Investment in the most probable scenario was calculated as 12465%. This calculation was based on the cloud-based solution provided by Cloudflare, a company that provides internet security services such as mitigation of DDoS attacks. With this, all expected risk is mitigated, for at least external actors. The modelling of internal actors such as employees (system managers) is not included in this model.

References

[1] Asosheh, A., & Ramezani, N. (2008). A comprehensive taxonomy of DDOS attacks and defense mechanism applying in a smart classification. *WSEAS Transactions on Computers*, *7*(4), 281-290.

[2] Cherdantseva, Y., & Hilton, J. (2013). Information Security and Information Assurance: Discussion about the Meaning. *Organizational, Legal, and Technological Dimensions of Information System Administration*, *167*.

[3] Zalando SE (2017). *Notes to the Consolidated Financial Statements*. Retrieved from https://annual-report.zalando.com/2016/fileadmin/user_upload/zalando2016_notes.pdf

[4] Amakai (2017). *State of the Internet / Security, Q2 2017 Report*. Retrieved from https://www.akamai.com/us/en/multimedia/documents/state-of-the-internet/q2-2017-state-of-the-internet-security-report.pdf

[5] Incapsula (2015). *Incapsula Survey: What DDoS Attacks Really Cost Businesses*. Retrieved from https://lp.incapsula.com/rs/incapsulainc/images/eBook%20-%20DDoS%20Impact%20Survey.pdf

[6] *E-commerce sites victim to DDoS attacks*
http://www.itwaynetwork.com/ecommerce-site-victim-to-a-ddos-attack/

[7] Mohurle, S., & Patil, M. (2017). *A brief study of Wannacry Threat: Ransomware Attack 2017. International Journal, 8(5).*

[8] *Cyber Security Assessment Netherlands, CSAN 2016, Nation Cyber Security Center, Ministry of Security and Justice the Netherlands*
https://english.nctv.nl/binaries/CSAN%202016_def_tcm32-145252.pdf

[9] Alexander Khalimonenko, Jens Strohschneider, Oleg Kupreev (2017). *DDoS attacks in Q4 2016*. Retrieved from https://securelist.com/ddos-attacks-in-q4-2016/77412/

[10] Verisign (2017). VERISIGN DISTRIBUTED DENIAL OF SERVICE TRENDS REPORT - VOLUME 4, ISSUE 1 – 1ST QUARTER 2017.
Retrieved from https://www.verisign.com/assets/report-ddos-trends-Q12017.pdf

[11] W^{3}Techs (2017). *Usage statistics and market share of CloudFlare for websites*. Retrieved from https://w3techs.com/technologies/details/cn-cloudflare/all/all

[12] Cloudflare (2017). *How large of a DDoS attack can Cloudflare handle?* Retrieved from https://support.cloudflare.com/hc/en-us/articles/200170216-How-large-of-a-DDoS-attack-can-Cloudflare-handle-

[13] Cloudflare (2017). *How much does the enterprise plan cost*
https://support.cloudflare.com/hc/en-us/articles/200170326-How-much-does-the-Enterprise-Plan-cost

[14] Sonnenreich, W., Albanese, J., & Stout, B. (2006). Return on security investment (ROSI)-a practical quantitative model. *Journal of Research and practice in Information Technology*, *38*(1), 45-56.