# WM0824 Economics of Cyber Security
# Assignment 2


Maria Simidžioski 4381319

Sam van Hooff 4247620

Tom Slooff 4492919


October 2019

# 1 Introduction

The problem owner of this security issue is an organisation that provides and manages an Autonomous System. An Autonomous System is a group of IP networks run by one or more network operators with a single clearly defined routing policy(Kühne, Nimpuno, and Wilmot 2003). This organisation provides Internet connection services to both individuals and other companies. These AS administrators can host websites for companies and also create websites themselves. An important characteristic of these Autonomous Systems is that they are all connected to each other through public network facilities or access points (Usman 2013).

The functions of these systems include providing information location or searching tools, storage of information and hosting websites, system caching and transmitting digital data from one point to another in the network (Usman 2013).

The organisation that administrates these Autonomous Systems is able to observe the traffic that is flowing into/out of the network and because of this they can detect possible malicious behavior.

(Rowe, Reeves, and Gallaher 2009) argue that these providers could be in a good position to cost-effectively prevent certain types of incidents. In order to detect malicious behavior, the AS administrator could implement additional filtering, create policies that the users must follow and provide security advice. Other technical measures that can be taken are to apply Intrusion Prevention Systems (IPS) and secure their DNS server (Pijpker and Vranken 2016).

# 2 Problem-owner

While the responsibility of the security and the maintenance of a website lies with a website owner, the website host or AS administrator, is responsible for the security and maintenance of its servers. Especially when multiple websites are hosted on a shared server, the security of one of the websites greatly influences the security of the other websites on the same server. Malware on one website can spread to other websites on the same server. Mainly because of this it is important an AS administrator takes an active approach in detecting and resolving issues of website defacement in its system.

## Risk definition

Defining the risk of website defacement for AS administrators is a bit difficult because typically the direct damage is done to the website owner in stead of the AS administrator. However there are several indirect costs as a result of website defacement. These costs include the costs as result of reputational damage and possible costs for violating regulations.

Reputational costs mainly consist of the cost of losing (potential) customers due to a bad name. For an AS administrator a solid reputation is exceptionally important, since there are a lot of other providers, supplying nearly the same product. Security is one of the areas an AS administrator can differentiate on.

Poor security practice of an AS can also negatively influence findability on search engines as Google. When a website gets defaced this may be noticed by Google algorithms or monitors, which may result in that IP address getting marked for spam and thereby all websites from this IP can get a lower pagerank from Google. Concretely, this means that when one website gets defaced, all websites on that server may suffer from a lower pagerank on Google. As pagerank on Google is very important for websites, and this may be monitored by these companies, this can result in complaints and extra costs for the hosting provider. It may also result in more severe costs such as companies switching hosting providers, but we assume this cost is encapsulated in the reputation loss costs.

There are several risk strategies the problem owner can choose to apply. These risk strategies are subdivided in 4 categories: reducing risk, accepting risk, avoiding risk or transferring risk.

*Accept risk*
Accepting the risk would mean to accept the situation as it is and take no action. In case of the security issue of website defacement this would result in the AS administrator leaving all detection and response to its customers and not taking any actions to prevent or minimize the potential incidents.
*Reduce risk*
In order to reduce the risk, the problem owner would need to take several preventive security measures. One possible measure is to inform and spread awareness

amongst its customers about the possible incidents regarding website defacement and how to mitigate those incidents. The AS administrator could also implement additional technical solutions such as intrusion detection systems and firewalls that would block malicious traffic from entering the network, this way the risk that a website would be defaced would be reduced and also the website owner would not be directly exposed to this risk.

*Avoid risk*

Avoiding the risk would mean to stop taking the risk all together. For an AS provider this would mean to stop doing business and stop providing its services.

*Transfer risk*

Transferring the risk would mean that the AS administrator will take an insurance that will make sure there are no costs for the website owner and AS administrator in the case that a website defacement happens.

# 3 Other actors & risk strategies

Besides the problem owner, the AS administrator, there are multiple other actors involved in, and influenced by, the security issue of website defacement. Typically those actors have a different function in the system as well as a (slightly) different perspective on the risk involved. In this section the different actors in the field and their definition of the risk of website defacement will be elaborated. Also, the risk management strategies an actor can follow are identified. Those strategies are subdivided in risk reducing, risk accepting, risk avoiding and risk transferring risk-strategies.

## 3.1 Customers of AS (website owner)

A customer of an AS administrator is defined as an entity paying the AS administrator for a domain on its net space, in other words a website owner. A website owner is the actor most directly affected by a website defacement of its website(s). A defaced website can impose a website owner with costs ranging from costs for recovery to costs for unavailability of the web service.

A website owner does have the ability to influence the security issue of web defacement, since the vulnerability to this issue greatly depends on configuration of a webserver, as well as the security controls in place.

**Risk definition and risk management strategies**

The risk of website defacement for website owners entails the the possible costs of recovery when a website is compromised and the costs of the unavailability of the service the website owner provides.

*Reduce risk*

Reducing the risk for the website owner would mean to improve the security of the website by implementing technical measures and also identify the possible adversaries that would want to deface the website and intentionally make the website less attractive for them.

*Accept risk*

Accepting the risk for the website owner would mean to leave the website as it is, not take any security measures against the possible website defacement incident and accept the costs related to this incident.

*Avoid risk*

Avoiding the risk for a website owner would mean to stop hosting the website to avoid any costs because if there is no asset, in this case a website, there cannot be a risk related to the asset.

*Transfer risk*

Transferring the risk for a website owner would mean to take out an insurance with an external party that will cover the costs in the case of a website defacement.

## 3.2 Regulatory authority

Regulatory authorities might have a great influence on the security issue of website defacement. By making new laws and enforcing them, regulatory authorities can influence the behaviour of different actors in the field. New laws might for example force AS administrators and website owners to take care of their security measures by imposing fines for negligence regarding their security. Also a legislator might decide to provide for more severe penalties for adversaries breaking the law. Increasing the risk for adversaries might cause some of them to stop.

**Risk definition and risk management strategies**

*Reduce risk*
Reducing the risk for a regulatory authority would mean to create laws and regulations that they will enforce on the AS administrators and/or website owners. If these AS administrators and website owners do not comply to these regulations fines should be imposed for not paying enough attention on the security. Regulatory authorities could also create regulations and penalties for adversaries.
*Accept risk*
Accepting the risk for a regulatory authority would mean to leave the AS administrators and website owners to work based on their own security principles and not impose any laws or regulations that affect the security of the Autonomous Systems and hosted websites.
*Avoid risk*
Avoiding the risk for a regulatory authority would mean to make rules that do not allow AS administrators to offer the service of hosting a website or prevent the potential website owner from creating the desired website.
*Transfer risk*
Transferring the risk to an external party would not be an option for a regulatory authority since the risk is not directly related to the regulatory authority and therefore there will be no direct negative consequences and costs.

## 3.3 Adversaries

Adversaries are the actors responsible for the defacement of websites. There are different types of actors with different motives. These motives can for example be political, patriotic, economic or terroristic. The goal of those adversaries is to make the targeted domain unavailable and/or broadcast their own message in the form of an alternative web interface.

The capability and motivation of the adversaries have a great effect on the security issue of web defacement, since the issue is the consequence of their actions. This actor will not be taken into account in further risk analysis, since their risk and their motives are opposite to the actors trying to mitigate the security issue of website defacement

**Risk definition and risk management strategies**

The risks that adversaries face when performing a website defacement are the possible costs that the adversary may have if the website defacement attack is not successful or the fines and penalties of the regulatory authorities if the identity of the adversary is discovered.

*Reduce risk*

The adversary could reduce the risk by creating a detailed and extensive plan on how and when to perform the attack and also collecting enough relevant information before the attack is performed.

*Accept risk*

The adversary will accept the risk by not taking any precaution measures when performing the website defacement attack.

*Avoid risk*

The adversary will avoid the risk by not performing the website defacement.

*Transfer risk*

The adversary will transfer the risk by engaging someone else to perform the website defacement attack.

## 3.4 Conclusion actor/risk analysis

Each of the previously mentioned actors has a different strategy that could be used to accept, avoid, reduce or transfer the risk related to a website defacement attack. The actors use different strategies because they all have different goals, assets to protect and costs involved in the potential incident of website defacement. The most similar strategies are used by the AS administrator and its customers, the website owners. The website owner has direct costs when a website defacement is performed on the website (asset). The AS administrator also has costs related to the server on which this website is hosted and the reputation because a website defacement attack would mean that the AS provider has no suitable security guarantee to its customers. On the other hand, the regulatory authorities have no direct costs regarding the risk but can try to reduce the number of adversaries that try to deface a website and also force the AS administrators and website owners to improve their security controls.

# 4 The metrics

Two metrics were defined in the previous report. One relating to the reaction time and quickness of AS operators to respond to defaced websites, and one to capture the amount of defaced websites of an AS operator in relation to their size. Thus the first metric aims to measure the capabilities of the AS provider, while the second metric aims to measure the prevalence of the security issue in the networks of the AS provider.

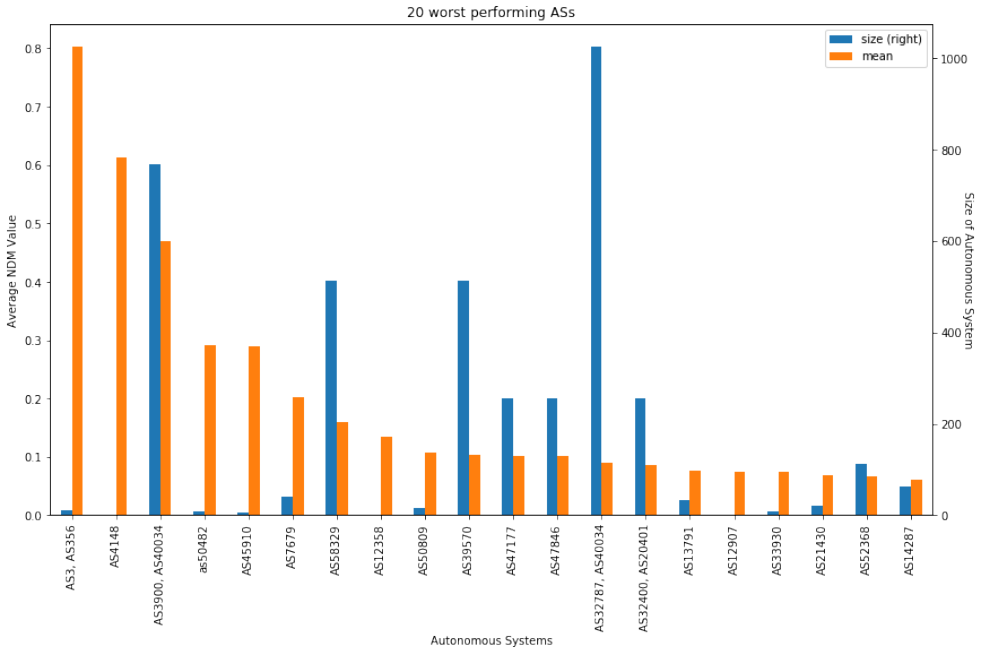



Figure 1: 20 ASs with highest average NDM value

Figure 1 shows the 20 Autonomous Systems (ASs) with the highest average normalized defacement count per month (NDM) value. One strength of the NDM is that it accounts for size, which means that large ASs don't have the disadvantage of a large count just because of their size. However, by normalizing the count this puts the smaller ASs at a disadvantage. This is because one attack in a small AS has a much larger impact on their NDM value. This can be seen when looking at figure 1, as all of the ASs with a high average NDM value have a small size compared to the mode of 4096. The mode is used here because of the few very large outliers on the right side.

To find ASs to compare using the metrics, it is therefore beneficial to account for the size component when comparing their average NDM value. Furthermore

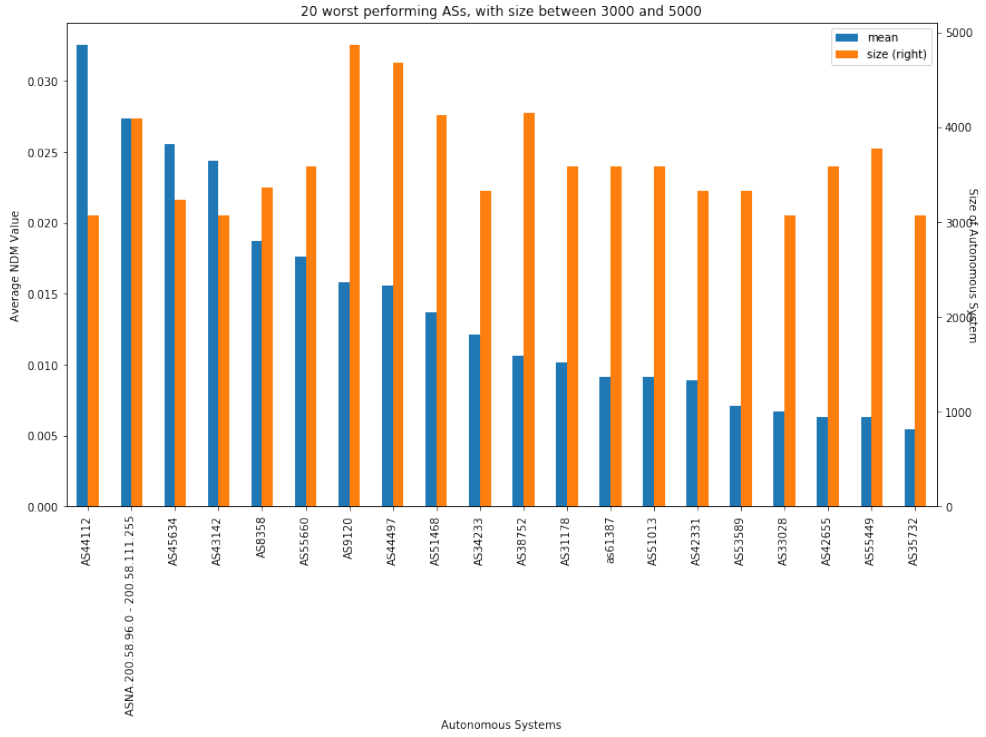



Figure 2: 20 ASs with highest average NDM value, with size between 3000 and 5000

taking a larger AS usually has the benefit of more incident data. Figure 2 shows the highest average NDM values for ASs with size between 3000 and 5000. 2 Ass with similar size, but different average NDM value are picked and evaluated further using the created metrics. AS44112 and AS35732 are the ASs with the highest and 20th highest average NDM in this size range, respectively. Furthermore they both have a size of roughly 3000. These ASs will be compared further.

Figure 3 shows how the NDM values for AS44112 and AS35732 over time. The figure shows there are trends in the number of attacks occurring for each AS, although AS44112 consistently has higher NDM values. For both ASs the number of attacks dropped after a small peak in the end of 2014. Especially before 2014, AS44112 has some months with a lot more attacks relative to AS35732.
The normalized defacement count per month (NDM) indicates the security level of the network of an AS provider. If the NDM has a low value, this means that there are few defacements occurring per month relative to the size of the network. This can be due to several reasons, of which the implemented security for the AS provider is one. However, it could also be due to factors such as attacker behavior or the content of the websites it is hosting. In order to compare the

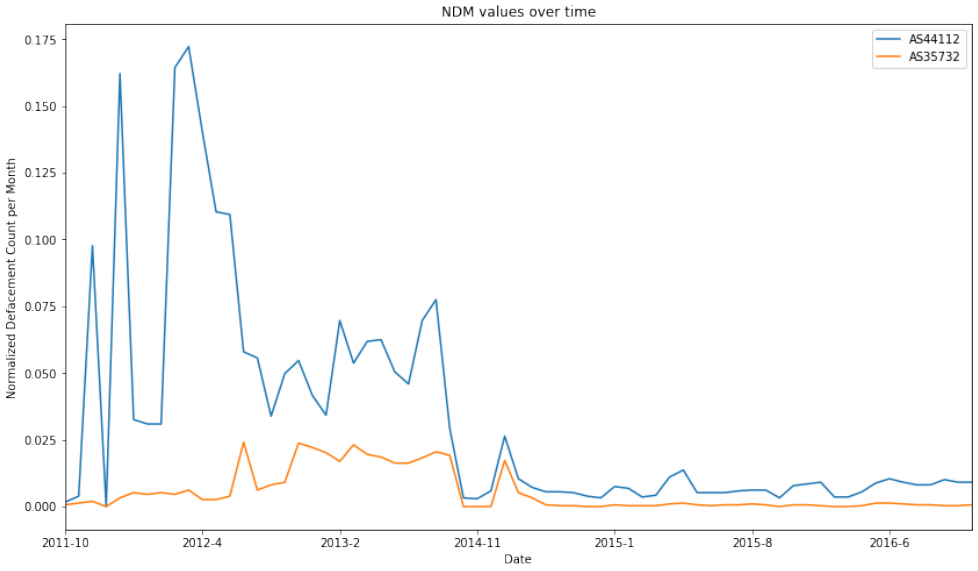
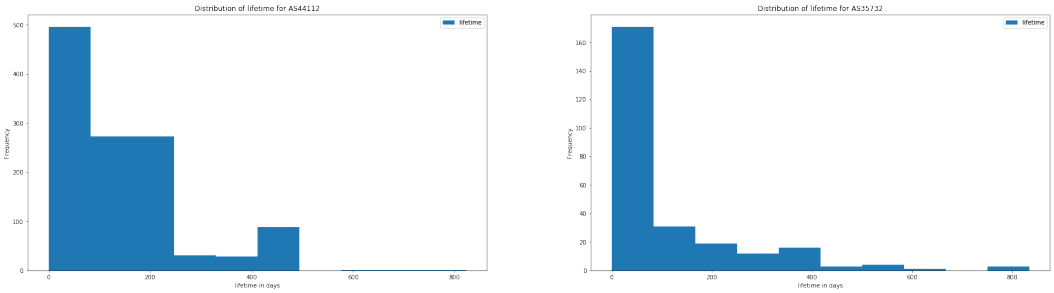



Figure 3: NDM Values over time for AS44112 and AS35732

relationship further, the distribution of response times can be used.




(a) Histogram of lifetime for AS44112

(b) Histogram of lifetime for AS35732

Figure 4: Lifetime histograms

Figure 4 shows the lifetimes of defacements in AS44112 and AS35732 respectively. The distribution is quite comparable between the two ASs. However, AS44112 handles a larger proportions of defacements after longer than 100 days. Whereas AS35732 handles most defacements in less than 100 days. It seems that both ASs have a few 'outlier' defacements which took more than 400 days to handle.

Based on these distributions it can be concluded that both suffer from some outlier cases which drag up their average lifetime. However AS44112 has a less clear exponential distribution and lets more cases linger for more than 100 days. Thus based on the given data, the security behavior of AS44112 seems to be a

factor in why their NDM values are higher than those of AS35732.

To conclude, the metrics designed in the previous report together form a framework to evaluate the level of security in an AS. Firstly by comparing the normalized amount of attacks per AS, and then evaluating the lifetime metric to estimate the involvement of the AS provider in this level of security. AS44112 was compared to AS35732 to show how the metrics can be used to find the involvement of the AS operator in the level of security, as compared to external factors.

# 5 Analyzing the risk strategy

In this section the chosen risk strategy will be analyzed and the costs and benefits of the chosen strategy will be discussed. Based on these costs and benefits, the Return on Security Investment (ROSI) will be calculated.

## 5.1 Costs involved in the strategy

AS providers have two kinds of costs regarding infected customers, those costs are the cost of implementing some security measures against botnets to prevent additional costs of blacklisting. The other cost is taking some action that will avoid costs of legal liability and customer calls (Asghari 2010).
The strategy that is chosen for the security measure by the Autonomous System administrators/providers is penetration testing. Two types of penetration testing exist, namely, black box penetration testing and white box penetration testing. Although penetration testing can be a valuable security measure for the AS administrator, it requires expertise, it can slow down the network response time because of vulnerability scanning and network mapping and it is also very labour intensive (Tracy et al. 2007). It is also possible that the system or parts of the system can be damaged when performing the penetration test and all these factors contribute to additional costs for the organisation. The following variables mostly affect the costs of penetration testing (Glover 2019):

- The complexity of the network and the environment
- The methodology that the pentester uses
- The experience of the pentester

- Whether the penetration test is is performed onsite or offsite
- If retesting is included in the costs
- The possible damage that can be done to the system because of the pentration test
- The slower response time of the network

Based on these variables the average cost of a penetration test can vary from $\$4,000$ to $\$100,000$ (Hacken 2019).

## 5.2 Benefits of applying the strategy

Applying penetration testing has several benefits for Autonomous System administrators. A penetration test is able to find weaknesses in a system and can provide evidence or disprove the perceived level of security in the organisation (Wilson 2003). Additionally, the reputation of the organisation can be protected if these penetration tests are applied adequately and redundant costs can be reduced.
(Tracy et al. 2007) argue that penetration testing is beneficial for an AS administrator because it applies similar or the same technologies that the adversaries use, penetration testing verifies if vulnerabilities exist in the system and verifies that these vulnerabilities are not only theoretical by demonstrating how the found vulnerabilities can be exploited and also tests the procedures and human factors related to the security of the system. All these aspect will contribute in the security of the organisation and help to maintain or even improve the reputation of the organisation.In short, the benefits that the AS administrator will have when applying penetration testing as the security strategy are the following:

- Verification that certain vulnerabilities exist in the system
- Use of similar or same technologies that the adversaries use
- Demonstration of how the vulnerabilities can be exploited
- Testing the procedures and human factors involved

## 5.3 ROSI calculation

*The Return on security investment (ROSI)* is (Sonnenreich, Albanese, Stout, et al. 2006):

$$ROSI = \frac{\text{(Risk Exposure * \%Risk Mitigated) - Solution Cost}}{\text{Solution Cost}} \quad (1)$$

The ROSI for the problem owner will be calculated over the timespan of 3 years. In the following sections the costs and benefits of the security solution will be estimated, and finally the ROSI will be calculated based on these estimations.

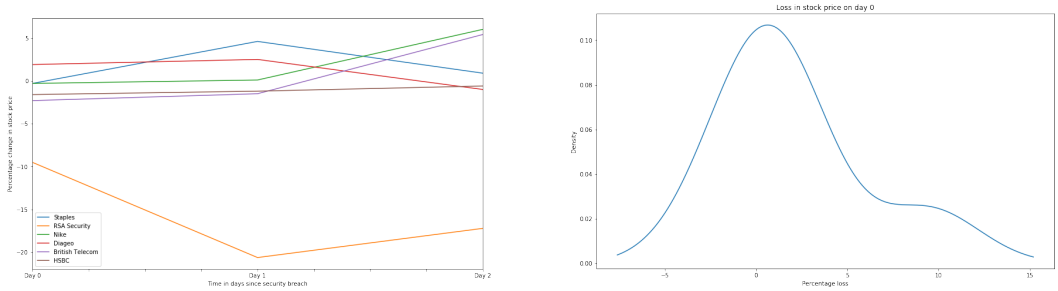
### 5.3.1 Costs of website defacement

As explained in section 2, the problem owners experience their costs in the areas of reputation loss and fines.

The cost of reputation loss is difficult to measure, as it in turn encapsulates many other costs such as customers going to competitors, the cost of regaining reputation, employees who become dissatisfied, and more. In a report by Oliver Wyman (Farha, Sekeris, and Hermansson 2017), the reputation loss is estimated using the difference between the expected stock value of the company, and the actual stock value after the incident. This is a direct way to analyze the impact of the reputation loss.

Garg, Curtis, and Halper 2003 analyze the impact of different types of hacks on the stock price of several large companies. Based on this, and some assumptions, an estimation can be made for the costs for the hosting provider. Some notes should be made on this data however. This data includes only large companies, and some were growing companies at the time, meaning that the impact of the security breach did not give the company a decrease in stock value. For example windows had customer information stolen through a defaced website, but still had an increase in stock price on all 3 days following the attack. Furthermore the data is from 1999-2001. Today, information spreads much quicker and 'outrage culture' can also lead to greater losses. Nevertheless this information can lead to a baseline on which to create a loss distribution.

Figure 5a shows how the stock increased or decreased for the companies who suffered a website defacement, for the 3 days following the incident. As can be




(a) Stock price fluctuations over time

(b) Stock price loss on day 0

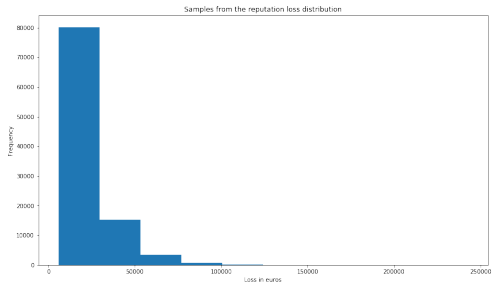
Figure 5: Effects of website defacement on market valuation

seen quite some of these companies still grew in stock value, but probably less than their usual rate of growth. Figure 5b shows the loss of stock price on day 0. This is a kernel density plot, so that the data can be generalized to a distribution. This distribution is a typical loss distribution, with a gamma distribution in the low costs, and some outliers which incur high costs. A probable loss distribution can be based on this data.

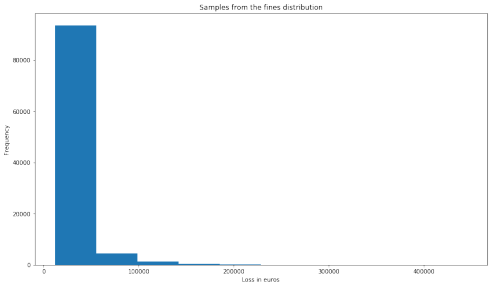
The costs of fines because of hosting providers not adhering to regulations are difficult to estimate, since these can't be found directly. However a hotter topic is the GDPR, and for this the fines are available. These fines maximums can be used as an indicator to which extent the EU will fine monitoring companies (Wolford 2019). Minor infractions will range up to 10 million euros, or 2% of the companies yearly revenue, whichever amount is higher. As website defacements are generally less severe than data privacy breaches, an estimate for the costs of poor monitoring is a maximum of 500 thousand euros. The same kind of loss distribution will be used as for the reputation costs, with the maximum being at 500 thousand euros.

To estimate the losses a gamma distribution is used with different parameters. The reputation loss is modeled by a gamma distribution with an alpha of 0.85, and a scale of 17000, shifted to the right with 6000. Samples can be drawn from this distribution. An example of some samples are shown in figure 6a.The costs of fines is modeled by a gamma distribution with an alpha of 0.2, a scale of 50000, shifted to the right with 12000. An example of some samples are shown in figure 6b.

For the creation of the first distribution, a model was fitted on the data of stock value decrease with a company value of 2 million. And the company with an increase in value was dropped. The parameters that were fitted were then adapted to get less random results for low sample counts. The fines costs are based on this, with the assumptions of upper bound costs mentioned earlier. However the alpha is decreased since we assume most fines will be on the lower end. To account for the lower alpha the shift is increased to 12 thousand.




(a) Samples from the distribution modeling reputation loss




(b) Samples from the distribution modeling fines

Figure 6: Distributions for both kinds of loss

### 5.3.2 Costs of the security solution

As described earlier, the costs of a penetration test typically ranges from 4 thousand to 100 thousand dollars. As the penetration tests will be largely very similar for the servers, the costs will mostly be on the lower end, with some outliers because of unforeseen costs such as network congestion. For this a special gamma distribution is used, namely the exponential distribution, where the alpha is 1. The scale is 7400 and it is shifted with 4000, to account for the minimum costs of the penetration test. This distribution can then be sampled for each server in the network. This will get the costs of the security solution. Some samples from the distribution can be seen in figure 7.

### 5.3.3 Benefits of the security solution

As the distributions of losses have been described, the benefits of the security solution can be defined using parameters of this distribution. Applying the security solution will result in less frequent website defacement. Additionally the impact of the defacements will also be less, because fines are less severe if there are fewer defacements, and reputation loss may be less severe if it is known that

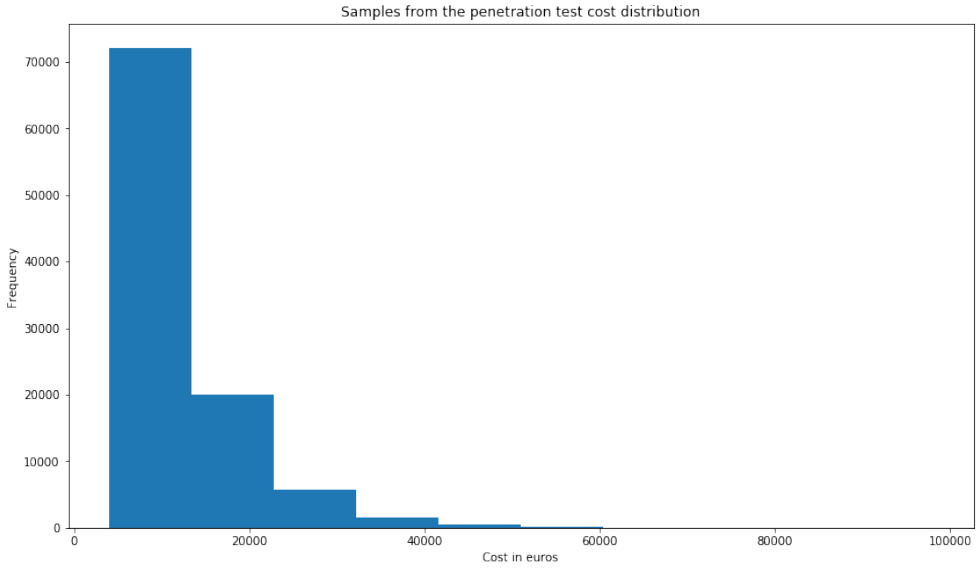



Figure 7: Samples from the distribution modeling costs of penetration testing

penetration testing was applied.

Figure 8 shows the distribution of the defacement count for 2016 for ASs in the given database, for ASs where less than 250 defacements occurred. Note that 97% of ASs had 250 or less defacements, but there were some severe outliers which obscured the distribution plot. Again a gamma distribution can be used. The distribution will be modeled by a gamma distribution with an alpha of 0.3 and a scale of 15.

Now the concrete effects of the security solution can be described in terms of the effects on the distributions. We expect the security solution can mitigate around 60% of the defacements that occur in an AS. Additionally the distribution of the costs of defacement will be shifted, with the distribution for reputation loss having an alpha of 0.75, and a scale of 13000, shifted to the right with 5000. And the distribution of the fines will be a gamma distribution with an alpha of 0.1, a scale of 50000, shifted to the right with 12000. Here we expect only the alpha to change as the size of the fines will be the same. This means that the higher value fines will occur less frequently.

### 5.3.4 Estimating the ROSI over a 3 year timespan

With the distributions estimated in the previous sections, the ROSI can be calculated over 3 years. Samples will be drawn from the distributions, which will

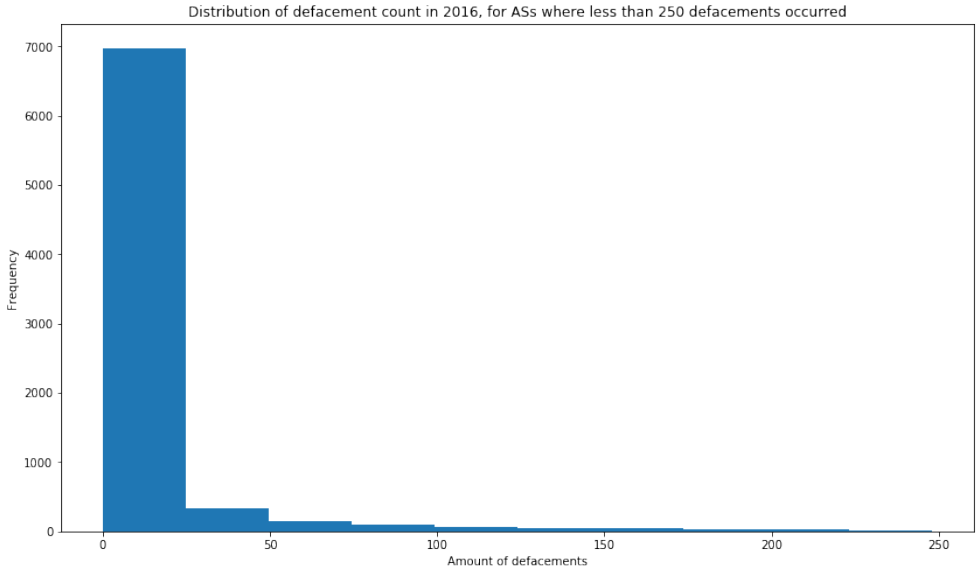



Figure 8: Distribution of defacement count for 2016, for subset of ASs

result in concrete numbers on which the ROSI calculation can be based.

In order to estimate the ROSI, firstly the amount of defacements will be sampled from the frequency distribution. This will give us 3 samples, which will be used for each year. The 3 samples are: [23, 1, 6]. The costs for these attacks can be calculated by sampling from the reputation loss and fines costs distributions, and adding these numbers up. This results in a cost of 20039680 euros over 3 years. This will be the baseline costs against which the security solution will be compared.

Now the benefits of the security solution can be calculated by, for each attack estimating whether it will be mitigated or not, and then sampling the costs from the adapted distributions or taking the costs as 0. This results in costs from attacks being 485807 euros with the security solution in place. Thus the benefits of the security solution can be calculated as 20039680 - 485807 = 19553873.

To complete the calculation of the ROSI, the costs of the security solution need to be calculated. The cost of pentesting each server is modeled by an exponential distribution with a scale of 7400, and shifted 4000. This distribution will be sampled from 4096 times, which is the mode of the network size in the dataset. This results in costs of 46768020 euros.

Finally, the ROSI can be calculated as:

$$ROSI = \frac{\text{Benefit of Solution - Solution Cost}}{\text{Solution Cost}} = \frac{19553873 - 46768020}{46768020} = -0.582 \tag{2}$$

# 6 Conclusion

In this paper we aim to quantify the risk involved in the defacement of websites. The problem owner, Autonomous System administrators, faces several possible losses induced by website defacement. These costs are mainly indirect of nature. The main losses for an AS administrator as a result of web defacement consist of loss due to a bad reputation and loss due to possible fines imposed by regulatory authorities.

Since there is no data available about the true costs of these factors, an estimation has been made. The cost for loss of reputation are estimated by using data about the impact of web defacement on the stock price of a company. For this calculation we have used a company with a market value of 2 million euro. The cost of fines are estimated by looking at the size of fines within the GDPR. The losses due to web defacement are highly uncertain. To capture this uncertainty in the analysis different gamma distributions are used.

To reduce the risk of web defacement, AS administrators could make use of penetration testing to improve the security of its servers. Most servers are vulnerable due to bad configuration. Pentesting would expose these vulnerabilities and enable patching. We have estimated that by pentesting all servers, 60% of the web defacement issues could be prevented. Also, in case a server does get attacked, the costs will generally be lower. The costs for Pentesting a server range between 4000 and 100000 euro per server.

Using this cost and benefit estimations the ROSI has been calculated over the timespan of 3 years. The result of this calculation is -0.582. This means it is financially unattractive to invest in Pentesting to mitigate the potential loss due to website defacement. Pentesting is a very effective mitigant against web defacement, but the costs are simply too high to make it financially rewarding on a large scale.

# References


Asghari, Hadi (2010). "Botnet mitigation and the role of ISPs". In: *Delft University of Technology. Nederland*.

Farha, Ramy, Evan Sekeris, and Daniel Hermansson (2017). *The Hidden Cost Of Reputation Risk*. URL: https://www.oliverwyman.com/our-expertise/insights/2017/jul/reputation-risk-management.html.

Garg, Ashish, Jeffrey Curtis, and Hilary Halper (2003). "The real cost of being hacked". In: *Journal of Corporate Accounting & Finance* 14.5, pp. 49–52.

Glover, Gary (2019). *How Much Does a Pentest Cost?* URL: https://www.securitymetrics.com/blog/how-much-does-pentest-cost.

Hacken (2019). *How much does Penetration Test Cost, or Price of your Security*. URL: https://hacken.io/research/education/how-much-does-penetration-test-cost-or-price-of-your-security/.

Kühne, Mirjam, Nurani Nimpuno, and Sabrina Wilmot (2003). "Autonomous System (AS) Number Assignment Policies and Procedures". In: *RIPE-263, http://www. ripe. net/ripe/docs/asn-assignment. html*.

Pijpker, Jeroen and Harald Vranken (2016). "The role of Internet Service Providers in botnet mitigation". In: *2016 European Intelligence and Security Informatics Conference (EISIC)*. IEEE, pp. 24–31.

Rowe, Brent, Douglas Reeves, and Mike Gallaher (2009). *The role of internet service providers in cyber security*. Institute for Homeland Security Solutions.

Sonnenreich, Wes, Jason Albanese, Bruce Stout, et al. (2006). "Return on security investment (ROSI)-a practical quantitative model". In: *Journal of Research and practice in Information Technology* 38.1, p. 45.

Tracy, Miles et al. (2007). "Sp 800-44 version 2. guidelines on securing public web servers". In:

Usman, Shuaibu Hassan (2013). "A REVIEW OF RESPONSIBILITIES OF INTERNET SERVICE PROVIDERS TOWARD THEIR CUSTOMERS'NETWORK SECURITY." In: *Journal of Theoretical & Applied Information Technology* 49.1.

Wilson, Marcia J (2003). "CISSP,"Demonstrating ROI for Penetration Testing (Part Four), 7 October 2003". In: *URL: http://www. securityfocus. com/infocus/1736*.

Wolford, Ben (Feb. 2019). *What are the GDPR Fines?* URL: https://gdpr.eu/fines/.