WM0824 Economics of Cyber Security
Assignment 3

Maria Simidžioski	Sam van Hooff	Tom Slooff
4381319	4247620	4492919

October 2019

1 Introduction

The problem owners plays a major role in the implementation of security strategies and mitigation of potential incidents. We will identify and discuss several actors that have a direct influence on the security level of the Autonomous Systems.

2 Actors

2.1 AS administrator

The AS administrator has the option to penetration test the servers on their network. This incurs high costs for the AS administrator as they often have large amounts of servers. The direct costs of hiring penetration testers is quite high, but there are also some indirect costs such as possible network congestion or downtime of servers. These indirect costs are determined by skills of the penetration testers, and the planning skills of the AS administrator. By taking a strategy such as letting other servers host websites while one website is tested, and only testing at night, will minimize these indirect costs.

The benefits for the AS administrator mainly are less defaced websites, and a better reputation. Customers will surely appreciate that servers are tested, if they incur no (large) costs because of it. And testing may also attract new customers. The fines that the administrator has to pay for not handling defacements properly may also become less, as there are less defacements.

The costs for the website owners are small depending on the skills with which the penetration testing is done. As mentioned previously, testing at night with other servers taking over the workload will lead to (almost) no costs for the website owners. The website owners do enjoy large benefits from this strategy. There websites will be more secure against defacements, so their risk is reduced without costs. How large this benefit depends largely on how secure the website was before the AS administrator pentested it.

The regulatory authorities do not experience any relevant costs or benefits from this counter measure.

The AS administrators of course have an incentive to apply this counter mea-

sure, as it does result in benefits for them directly (and indirectly). However it is important to consider how strong this incentive is, since the benefits may be outweighed by the costs. In this case the incentives are not very strong, as the benefits may be quite high, the costs are even higher.

The role of externalities in this counter measure has an impact on the incentive for the AS administrator to apply it. The AS administrator bears almost all of the costs, since they must hire the penetration testers and plan it. But the benefits for a large part go to the website owners who now have more secure servers to rely on. This may in return result in more satisfied and loyal customers which may be a benefit for the AS administrator, but this is not the case for all customers. A lot of customers might not care. Thus there is no strong incentive for AS administrators to apply this counter measure.

2.2 Website owners

Pentest their website

Website owners have the option to penetration test their own website, which results in a more secure website. For this measure the website owners experience most of the benefits, and they also bear all the costs. Penetration testing is an effective way of securing your website, but it is also expensive. Through penetration testing the website owners may greatly reduce their amount of defacements. This is a benefit for the website owner, but also for the AS administrator. AS administrators may be tasked with dealing with website defacements by regulatory authorities, which mean costs for them. Additionally the AS administrator may get less fines for this, and may get a better reputation. However, on the scale of one website getting secured these benefits are practically non-existent. The AS administrators can also experience costs from the penetration test, depending on how it is executed. If the penetration test involves some automatic scanners, this may be a large load on the network which causes costs for the AS administrator. The regulatory authorities do not have any costs or benefits because of this counter measure.

The incentive for the website owner to deploy this counter measure depends on several factors. Important ones are the cost of the penetration test, and how effective it is at mitigating defacements. But for a company to consider this counter measure, characteristics of the company itself may be even more important. For example small companies will probably care less about this attack, as

they are less likely to be targeted. If the company does not have a reputation which attracts activists, they may not consider website defacements as relevant. The costs in relation to the budget of this company may be too large. Additionally, the costs for smaller companies are not as large as for big companies which have thousands of visitors every day. Thus the incentives depend largely on characteristic of the business and the business environment it operates in, in addition to the direct costs and benefits of the counter measure.

The previous paragraph described the incentives for the website owner to deploy the counter measure. The externalities involved in the counter measure were not mentioned, as these do not play a large role in this counter measure. This counter measure has the externality of some benefits for the AS administrator. However, the majority of the benefits are enjoyed by the website owner itself, meaning that externalities do not deter the website owner from deploying this counter measure. There are also no relevant external costs to society or the environment which stop the website owner from deploying this counter measure. There are external costs for the AS administrator, if the penetration test is not carefully executed. But these costs most probably do not come back to the website owner, so they may not care about it.

2.3 Regulatory authorities

Regulatory authorities could impose stricter regulations as a countermeasure for the security issue of webdefacement. They could for instance designs certain standards to which the industry needs to adhere. It highly depends on this design and on the decision on who is held liable, how the costs and benefits are distributed. An option would be that the regulatory authorities introduce new laws, which force an AS administrator to maintain a certain security standard on its network. They could for example make new law which states that the network an AS is governing never may contain more than x defaced websites. Or a law that defaced websites should be resolved within an hour. If an AS administrator fails to comply, the regulatory authority could impose a fine. Of course regulatory authorities could also choose to hold the website owners responsible for a defaced website, in which case the costs for fines are for the website owner instead of the AS administrators.

It is difficult to asses the distribution of costs and benefits of regulation among

different actors. Regulation often produces costs and benefits for a society as a whole (Renda et al. 2013). Of course direct costs such as implementation costs

3 Type of actor

In this section the type of actor that is relevant for this scenario will be proposed and the underlying factors that cause a variance in the metrics will be discussed.

The type of actors whose security performance is visible are the

3.1 Underlying factors

The underlying factors that can cause a variance in the metrics are the following (Van Eeten et al. 2010):

- The country where the AS is located
- The size of the AS company or network
- The number of customers
- The type of websites that the AS hosts
- The costs spent by the AS on security (investment of the company)
- The legal implications and regulations that hold for the AS
- The competition of the AS
- The costs of the customer support that the AS provides
- The behaviour of the customers (security awareness, online activities)
- The education and income level of the customers
- The reputation of the AS

3.2 Data collection

The technology index[1] will be used for the purpose of gathering additional data to get better insights into this problem. The technology index is a country-level statistic based on factors like company spending on R&D, and personal computer and internet penetration rate, among others. We expect countries with high technology index, meaning a larger adoption of technology and more of the population being exposed to the internet, to be a greater target for website defacements.

As a measure for population education, the education index[2] is used. The education index uses the average amount of years of schooling and expected years of schooling. With a more educated population we expect a higher level of security and thereby a lower defacement count.

3.3 Statistical Analysis

In this subsection a statistical analysis will be performed in order to explore the impact of these factors on the metric.

3.3.1 Normalized Defacement count per Month correlated with technology index

Take ASs with size > 1000 to avoid large NDM values just by low size. Take average NDM value per AS and correlate it with the technology index for the country it is in. See how high the correlation is.

3.3.2 Normalized Defacement count per Month correlated with education index

Take ASs with size > 1000 to avoid large NDM values just by low size. Take average NDM value per AS and correlate it with the education index for the country it is in. See how high the correlation is.

[1] https://www.nationmaster.com/country-info/stats/Economy/Technology-index
[2] http://hdr.undp.org/en/content/education-index

4 Conclusion

References

Renda, A et al. (Dec. 2013). *ASSESSING THE COSTS AND BENEFITS OF REGULATION*. URL: https://ec.europa.eu/smart-regulation/impact/commission_guidelines/docs/131210_cba_study_sg_final.pdf.

Van Eeten, Michel et al. (2010). "The role of internet service providers in botnet mitigation an empirical analysis based on spam data". In: TPRC.