Economics of Cyber Security

Assignment Block 3

Marco Dijkslag	Mathay Kahraman	Yoep Kortekaas	Sam Witt
s1743716	s1724665	s1719734	s1672509
4985028	5124182	4984595	5100356

October 7, 2019

1 Introduction

To combat the DDoS attack security issue, this paper will introduce an analysis of the entity responsible for the problem and the strategies that this entity follows or can follow to deal with it. In our last research paper[6], the DDoS security issue is explained, including an analysis of the actors and ideal security metrics that can be associated with DDoS attacks. The main actors were determined to be companies offering online services, people with IoT devices in their homes, manufacturers of IoT devices, criminals and governments. New metrics were also derived from an IoT honeypot dataset, to help identifying the problem and constructing methods to solve it.

2 Problem Owner

When defining the problem owner, it is quite essential to first explain what a problem owner is. The problem owner is responsible for an individual problem. The problem owner oversees the handling of the problem, bringing in analysts and specialists as needed to handle the problem. The problem owner is responsible for seeing that analysts and specialists bring the problem to a close[5].

As described in our previous paper[6], DDoS attacks are mostly due to having large botnets that gather new malicious devices by scanning the internet and attempting a lot of default credentials on potential vulnerable devices. These devices are vulnerable, since users do not change the default credentials and because manufacturers do not require to change the default credentials.

This brings us to the point where we have to describe who the problem owner is. One could discuss that the problem owner is the user of the device, since (s)he did not change the default credentials. On the other hand one could argue that the problem owner is the manufacturer of the vulnerable device, since he could require that users must change the default credentials on the first boot. We decided that the problem owner is the manufacturer of the device, since they are in first place responsible that the default credentials must be changed on first boot and they are responsible to repair vulnerabilities of their devices.

3 Differences in Performance

To measure the performance of security in IoT devices, the frequency of the most used login credentials in attempt to gain access to the IoT honeypot device, has been plotted over time. In figure 1, the usage of the different credentials is visible in percentages. The login attempts have been measured from the 1st to 31st July 2016, then jumping to the 29th of August 2016 until the 13th of September 2016.

For manufacturers, these are useful statistics, as they provide proof that default credentials are not safe, and are being abused by attackers to gain unauthorized access to IoT devices. In

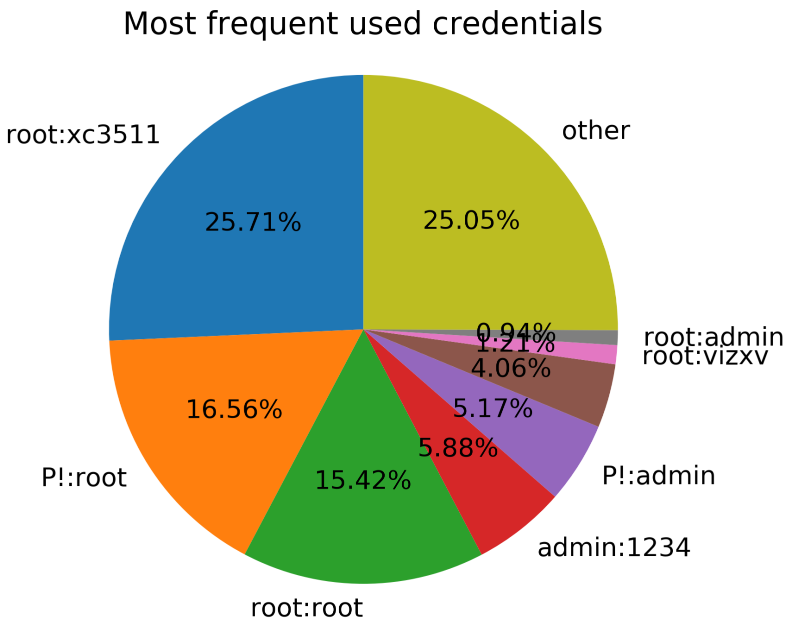

Figure 1: The credentials used by attackers to try to log in to devices.

figures 2 and 3, it is visible that at first, these credentials were not effective or not yet used to gain access to devices, but for both at some point, their usage spikes immensely. This means that from that point on those login credentials were discovered to be highly effective. In figures 4 and 5, we see credentials that were already being abused before the measurements started. The usage of root:xc3511 signals towards a specific device, namely the IP cameras of the Chinese vendor XiongMai Technologies[6]. This shows the danger when such a default password leaks.

We see that the login attempts get less frequent the longer they are known. This is because of how the botnets work. When a new device gets infected, it scans for new targets to attack, and attacks vulnerable devices it finds. But the more vulnerable devices, of a specific type with specific login credentials, have been compromised, the less new devices of this type will be available to be infected. This could explain the reduction in the frequency once time progresses.

It is also known that the only port scanned on those devices, is port 23 [6]. This is a port that is often not needed for the service of the device.

From this data, we can clearly see that IoT device manufacturers are not performing well with respect to equipping their devices with the necessity of secure login credentials. There is no data on specific device types and specific manufacturers, but in general it can be said that there is a lot of improvements to be made.

4 Risk Strategies for Problem Owner

To reduce the security issue that was measured and described in the previous section the problem owner can implement several risk strategies. Here we describe four of these risk strategies and the relation to the type of risk strategy that can be implemented by the problem owner.

The first strategy that can be implemented is for a user on installing an IoT device, i.e. an IoT device manufacturer, to make changing the default username and password of the device obligatory. Moreover, the user should not be able to use the device without changing it. Also during the installation of the device one can make the user aware that changing it is important and what could happen in case this procedure was not executed. This way we can also avoid that a lot of users set an easy password. On the one hand we argue that this risk strategy is

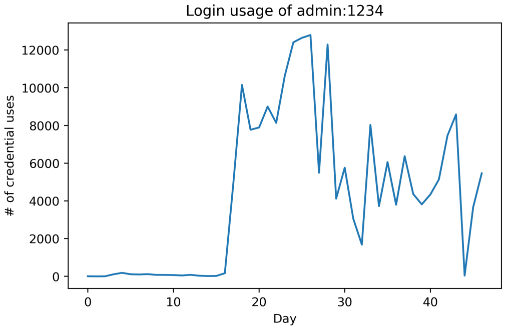

Figure 2: The usage of admin:1234 as login credentials over time.

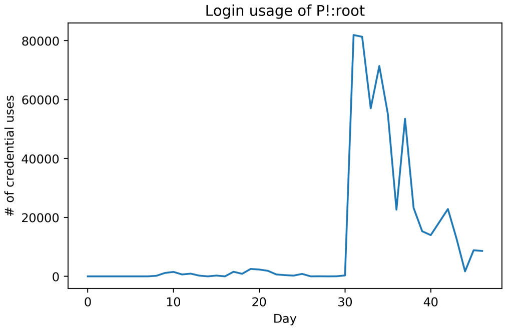

Figure 3: The usage of p!:root as login credentials over time.

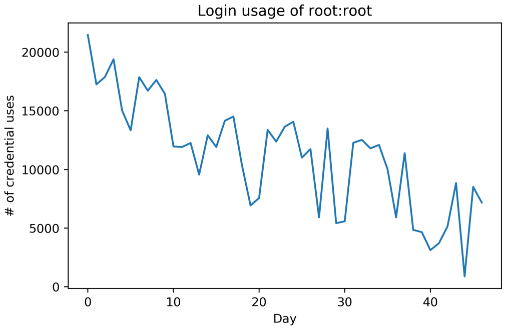

Figure 4: The usage of root:root as login credentials over time.

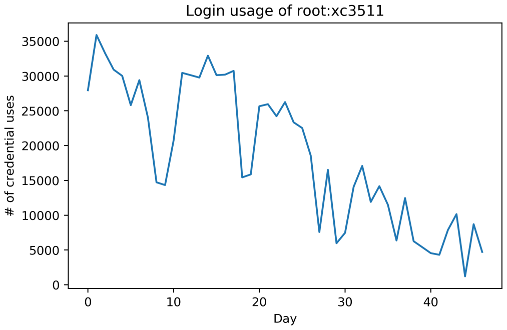

Figure 5: The usage of root:xc3511 as login credentials over time.

of type *risk reduction*, since the manufacturer implements it to force the user to set a username and password. On the other hand if the manufacturer closes an agreement with its users, i.e. they are responsible for their insecure devices, we would argue that it is of type *risk transfer*.

A second strategy that can be implemented is to close the telnet (port 23) on the device. This port is often abused by botnets to infect other devices over this channel. For the average costumer there is no need to leave this port open, whereas most customers would not know there exists such a port, what such a port is in general or what it can be used for. We argue that this risk strategy relates to *risk reduction*, since the manufacturer takes responsibility to mitigate this risk.

Lastly, the manufacturer of IoT devices can implement a strategy to provide long-term-support (LTS) for their devices. They can bring out patches and let users update their devices when they know there is a malfunction or when a security flaw has been discovered. Also by providing updates to their customers it can be used as a method to set a device back to its factory settings (or any other preferable state) when it is discovered it got infected by a botnet. Furthermore, an option to auto run updates for these devices makes it easier for the user to keep their devices secure and the manufacturer does not have to encourage users to update their devices, since users can be reluctant to update their device. We argue that this risk strategy corresponds to the type *risk reduction*, since the manufacturer takes responsibility to mitigate this risk.

Currently we have no risk strategies that belong to risk acceptance or risk avoidance. We could argue if the manufacturer is forced to implement a strategy, e.g. to comply with regulations, to provide security for its customers and therefore does not sell there devices anymore in a certain country it would be *risk avoidance*.

5 Other Actors

Next to the problem owner, the manufacturer of the IoT device, there are other actors that can influence the security issue we measured in our previous assignment. In this section we will define these other actors, and why this issue is relevant to them.

Government

The first actor we will discuss is the government. There are several reasons why this issue is also relevant to governmental institutes. The first and most important reason is that mostly critical parts of a nations infrastructure, such as governmental institutes[7], but also banks[3] are popular DDoS attack targets. Since these targets are a critical part of the national infrastructure, it is in the government's best interest to protect these assets from DDoS attacks.

Another reason for governments to partake in reducing unsafe IoT devices (and thereby reducing DDoS attack strength) is to prevent certain criminal activity. Next to using DDoS to disrupt critical services, it can also be used by criminals to cover up other shady activities like data theft[8]. Reducing (the strength of) DDoS attacks can lead to less attacks, or at least less obfuscation of the actual attacks, which in the end will lead to an reduction in organised IT crime.

Major online platforms

The second actors we will discuss are major online platforms. Under major online platforms we consider social media platforms such as Facebook and Twitter, but also online retailers like Amazon, hosting providers like OVH, DNS providers like Dyn and any other large company that gets the majority of their business from online services. The main reason why these platforms should be interested in reducing the security issue is that DDoS attacks threaten their main source of income. These platforms can only earn revenue when their services are available, and DDoS attacks undermine the availability of their services. Repeated unavailability of online services can even lead to permanent loss when customers switch to a different platform with better up-time.

For hosting and DNS providers this risk of permanent losses is even larger, since the unavailability of their services can lead to unavailability of other online services. An example of this happening is when DNS provider Dyn got hit by a 1.2 Tbps DDoS attack in 2016, leading to the unavailability of major online platforms like Twitter and Netflix[10].

IoT device owners

The last actor we are discussing are the owners of the IoT devices. Reducing the security issue is relevant to them too for a couple of reasons. The first reason is that having a vulnerable device in their private (home) network, gives an attacker entry to the private network. This means that devices that are normally not visible to the internet, now can be reached, and possibly compromised, by an attacker. So reducing the security issue means that IoT device owners have less risk of other (personal) devices getting hacked.

A second reason why reducing the security issue is relevant for IoT device owners has to do with the functioning of the IoT device. When such an IoT device is compromised, an attacker (usually) has full control over the compromised IoT device, meaning they can execute whatever action they like. This can lead to an increase in power usage, meaning that the usage of the IoT device is more inconvenient. A more serious issue is that an attacker can make the IoT device unresponsive, or even change the functionality of the device, e.g. giving back incorrect temperature readings for a temperature sensor.

Now that we have an idea of what kind of other actors this security issue is relevant for, we will discuss in the next section what kind of strategies these ”other actors” can exercise to reduce the security issue at hand.

6 Risk Strategies for Other Actors

The previous section describes which other actors there are. This section will describe what kind of risk strategies these other actors can adopt to tackle the problem of DDoS attacks.

6.1 Actors with different strategies

The first other actor that has been defined are governments. Governments are often target of DDoS attacks[2] and to reduce the number of attacks (or magnitude) they could start an awareness campaign under their citizens such that the owners of potential malicious devices are aware of the risks of not changing the default credentials and updating their devices such that they are always running at the latest released software version. This way the government can reduce the risk of DDoS attacks.

The second other actor are the IoT device owners. As described in the previous paragraph, these IoT device owners should change the default credentials of their IoT devices and enabling auto-updates on their devices such that their devices are always running on the latest released software version. This way IoT device owners can reduce the risk of their IoT devices becoming part of a botnet.

The third strategy is based on two different actors: governments and major platform owners like Google and Facebook. To reduce the risk of being a target of a DDoS attack, these two actors could put pressure on manufactures of vulnerable IoT devices such that they invest more resources in the security of their IoT devices.

6.2 Changes in strategies

Although there exist some campaigns by governments to raise awareness for people's online security, we are not aware of a campaign that is targeted at people's IoT devices. Meaning there is no risk strategy in place from the government perspective to tackle the problem of IoT devices getting infected by botnets.

Most users do not change the default credentials of their IoT devices and are not aware of the risks involved in not doing this. Meaning there is no risk strategy in place for the customers of these IoT devices regarding the security of the device, and no intention to do so either. If the users are aware of the security issues of their IoT devices they are more likely to keep them up-to-date and change the default credentials.

Major platform owners could implement the strategy of putting pressure on manufacturers of IoT devices to keep the devices security up-to-date, since otherwise they might have no intention for this. We are not aware of existing major platform owners that actively put pressure on manufacturers to keep their devices secure.

7 Return on Security Investment

The risk strategy that will be discussed in this section is the risk strategy of major platform owners. These major platform owners are a high class target for DDoS targets and that means that they are often targets of high scale DDoS attacks. Their return on investment is likely to be high if they can prevent losses due to DDoS attacks. For our ROSI calculation we will focus on costs and benefits in the Netherlands, since we could find the most literature regarding costs and benefits for DDoS attacks and campaigns in the Netherlands.

7.1 Costs

To decrease the amount of DDoS attacks the major platform owners could start an awareness campaign. An awareness campaign obviously costs money. To determine the amount of costs to start and maintain a campaign we have taken a look at the cost that SIRE[1] has when creating a campaign in the Netherlands. In 2011 they have created four large campaigns. The total costs of these four campaigns were 9.5 million euros[1], meaning that the average costs of these four campaigns is roughly 2.4 million euros.

[1] SIRE is a Dutch organisation that creates media campaigns regarding important societal issues[9]

To calculate the average DDoS attack cost for businesses is quite difficult. Fortunately, NBIP has done a research in this area in the Netherlands and came to the conclusion that in total there was damage of 425 million euros and the amount of damage per attack is approximately 1.8 million euros[4]. From this we can conclude that in 2018 there was an average attack frequency of 237 attacks.

Previously defined costs are related to direct costs such as sum of expenses for acquisition and the deployment of the awareness campaign. Other types of costs are called indirect costs, which consists of productivity loss for example. To define the productivity loss due to creating an awareness campaign, we have to define how many employees of each company are working with creating the awareness campaign.

For the awareness campaign, the company needs to assign at least one person as a contact point for the campaigning bureau. Assume that this new function incurs a productivity loss of 60 euros each hour (s)he is working with the campaign instead of his/her own tasks. Next we need to determine the amount of hours (s)he is working on the campaign. Assume that creating the awareness campaign takes three months (roughly 17 weeks). Every week the employee is working one working day (8 hours) on the awareness campaign. This can be different types of tasks: discussing the template of the campaign and which TV channels to display the campaign for example. In total this means that the productivity loss of assigning this employee to the campaign is $17 * 8 * 60 = 8160$ euros. However, if more companies join the awareness campaign, not every company needs to assign a person to work on this campaign for the duration of the campaign. We estimate that the campaigning bureau that creates the campaign only needs one industry representative for expert feedback.

Concluding, we estimate that the total cost for the campaign therefore is $2.400.000 + 8.160 = 2.408.160$

7.2 Benefits

There are two approaches to calculate the benefits of this awareness campaign: the approach where there are less DDoS attacks due to having less infected devices in a botnet and the other approach is that the DDoS attacks that are still there are less powerful than before and thereby easier to reflect.

The benefits when there are less DDoS attacks performed, is quite easy to calculate: each DDoS attack less, then in the same period before, is a saving of averagely 1.8 million euros. To define how much less DDoS attacks there are after the awareness campaign compared to before is difficult to calculate. We believe that a DDoS campaign can mitigate around 5% - 20% of the DDoS attacks we see now.

To calculate the decrease in strength of DDoS attacks we have to make a guessing like described in the previous paragraph. We believe that a successful DDoS campaign can decrease the strength of DDoS attacks between 5% and 25%.

7.3 Result

In order to calculate the RoSI value, we use the following formula:

$$RoSI = \frac{ALE_0 - ALE_s - c}{c}$$

To calculate the RoSI, we need to calculate the ALE$_0$ and the ALE$_s$. ALE stands for Annualised Expected Losses and is calculated as follows:

$$ALE = \text{Impact (Unit)} \cdot \text{Probability (Annual)}$$

First we calculate the ALE$_0$, this stands for the ALE without the security measures in place. The impact will be set to the average costs of a DDoS attack, which is 1.8 million euros. The probability will be set to the amount of attacks (237) divided by the amount of targeted .nl domain names (770.000) which is roughly 0.03%. This results in $ALE_0 = ((237/770.000) * 1.800.000) \approx 554$.

Next to the ALE_0 we also need to calculate the ALE_s, this is the ALE with the security measures in place. As described in the previous section the amount of DDoS attacks will decrease probably with 20% in the best case, which results in a total amount of $(237 * 0,8) \approx 190$ DDoS attacks and which will result in an average cost of $(1.800.000 * 0,75) = 1.350.000$ euros per DDoS attack since we estimated in the best case 25% cost reduction of attacks. The probability of being attacked by a DDoS attack is set with these values to $((237 * 0.8)/770.000) \approx 0.025\%$. This results in $ALE_s = (((237 * 0.8)/770.000) * (1.800.000 * 0,75)) \approx 332.42$. In the worst case, with 5% DDoS attack reduction and 5% DDoS attack cost reduction, we have an ALE$_s$ of ≈ 500

The last step is to calculate the RoSI, which stands for Return on Security Investment and is calculated by: $\frac{ALE_0 - ALE_s - c}{c}$. The c stands for costs and is defined in the *costs* section above by 2.4 million euros for the direct costs. The other costs we have are the indirect costs, which consists of the productivity loss which is 8160 euros. Which makes the total costs to 2.408.160 euros. This results in a worst-case RoSI of: $\frac{554-500-2.408.160}{2.408.160} = -0.9999775.$, and a best-case RoSI of $\frac{554-332.42-2.408.160}{2.408.160} = -0,999907$.

The result of the RoSI is negative, which means that it is not worth for a single company single-handedly to invest in a security awareness campaign. This can be easily explained, because the costs of an awareness campaign is rather large compared to the in risk of a DDoS attack and the amount that a DDoS attack costs. To let the RoSI result in a positive value it would be smarter for companies to invest together in one awareness campaign such that the costs for the companies decreases.

In Figure 6 we plot the RoSI values in the case that more companies participate in the awareness campaign. We see that in the best case (20% less attacks, and attacks cost 25% less) that we need 10867 companies to participate in order for the investment to start becoming rational. In the worst case (5% less attacks, and attacks cost 5% less), we need 44582 companies to participate in order for the investment to start becoming rational.

When creating the awareness campaign with all the targeted devices (770.000) the total costs will decrease to $(2.408.160/770.000) \approx 3,12$ euros. This results in a RoSI of $\frac{554-423-(2.408.160/770.000)}{(2.408.160/770.000)} \approx 69.86$, which means that creating an awareness campaign is a rational choice.

Another option that we can look into is to calculate the ALE over more than one year, since it maybe might not be rational to invest in awareness if we look only at next year, but it might be rational if we look at the returns over multiple years.

7.3.1 Multiple Years

In order to look at the benefits over multiple years, we created Figure 7. To calculate the RoSI over multiple years, we multiplied the ALE$_0$ and ALE$_s$ by the years and keep the costs fixed, so for example when we calculate the RoSI over 3 years, the ALE$_0$ will be set to $554 * 3 = 1662$ and the ALE$_s$ will be set to $423 * 3 = 1269$. Looking at Figure 7, we can see that even if we look at multiple years, it is not rational for a single company to do an awareness campaign, since it will take around 10.000 years for the investment to become rational.

7.3.2 Upper & Lower Bounds

The previous subsection defined multiple percentages by which the amount of attacks will be decreased (10%) and the average costs of a DDoS attack will be decreased (15%). Figure 6 shows nine lines in which the amount of attacks will be decreased from 5% (lower bound), 10% and 20% (upper bound) and in which the average costs will be decreased from 5% (lower bound), 15% and 25% (upper bound). Taking these kind of different values for the percentages means that the amount of uncertainty about these parameters will decrease, since we take also the lower and upper bound into consideration in the calculations. This shows that even if the percentages of decreased attacks and costs are as low as the lower bound, if enough parties participate, the RoSI value will be positive.

8 Conclusion

In this report we have defined and discussed several security investment & management related concepts regarding our security issue. In section 2 we presented the IoT device manufacturer as problem owner, since we think that it is the manufacturer's responsibility to release security

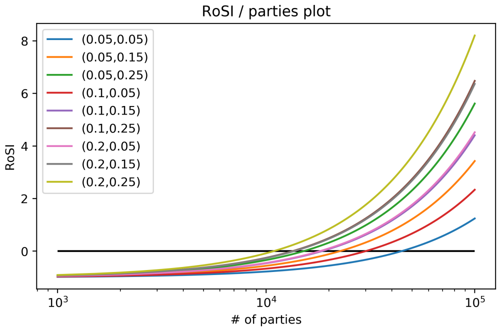

Figure 6: Plot describing RoSI vs. number of parties that share the costs. (p, q) describes the percentage of attacks mitigated(p) and the percentage of lowered DDoS costs (q)

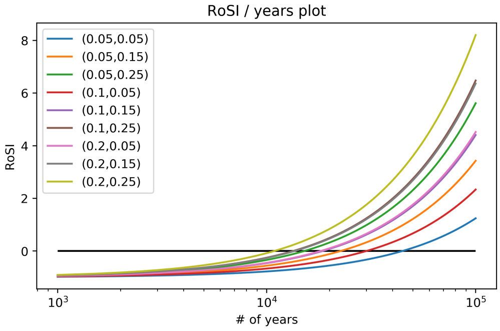

Figure 7: Plot describing RoSI vs. years that the campaign's effects are noticable. (p, q) describes the percentage of attacks mitigated(p) and the percentage of lowered DDoS costs (q)

patches for their devices, and make sure IoT device owners change default credentials on first boot.

In section 3 we discuss our findings in differences in performance using the most frequently used credentials in attempt to gain access to IoT devices. They provide proof that default credentials are not safe, and are being abused by attackers to gain unauthorized access to IoT devices. We discussed that IoT device manufacturers are not performing well with respect to equipping their devices with the necessity of secure login credentials.

In section 4 we discuss which risk strategies the problem owner (the IoT device manufacturer) can take to reduce the security issue. We discuss three different risk strategies, namely changing default credentials on boot, closing Telnet/remote access ports and lastly providing long term (security) support for IoT devices.

In section 5 and section 6 we discussed which other actors, next to the problem owner, (should) have interest in, and can partake in reducing the security issue. We identified the government, major online platforms and IoT device owners as potential other actors. Risk strategies that they can exercise are (among others) doing awareness campaigns, and putting pressure on IoT device manufacturers to secure IoT devices better.

Finally in section 7 we took one of our risk strategies, and we computed the *Return On Security Investment (RoSI)* score for that strategy. We chose to compute the RoSI for the awareness campaign strategy, looking specifically at the Netherlands since most of our sources regard the Netherlands. The result of our RoSI calculation is that the awareness campaign gets a score of -0.99 for when a single company funds the entire awareness campaign. When the cost of the campaign is distributed over all in 2018 targeted companies, the RoSI score of the risk strategy is +69.86.

References

[1] Jaarverslag 2011. https://sire.nl/wp-content/uploads/2017/10/2011-2.pdf, Aug 2012. Accessed: 2019-09-30.

[2] Cyber attack shuts down many government websites in finland. https://yle.fi/uutiset/osasto/news/cyber_attack_shuts_down_many_government_websites_in_finland/10350316, Augustus 2018. Accessed: 2019-09-27.

[3] Nieuwe ddos-aanval op abn amro, ing, rabo en belastingdienst. https://nos.nl/artikel/2214537-nieuwe-ddos-aanval-op-abn-amro-ing-rabo-en-belastingdienst.html, Jan 2018. Accessed: 2019-09-29.

[4] N. Boerman, M. Henneke, G. Moura, G. Schaapman, and O. de Weerdt. The impact of ddos attacks on dutch enterprises. https://www.nbip.nl/wp-content/uploads/2018/11/NBIP-SIDN-DDoS-impact-report.pdf, Nov 2018. Accessesd: 2019-09-30.

[5] IBM. Role: Problem owner. https://www.visioline.ee/itup/itup/roles/problem_owner_3556C72.html. Accessed: 2019-09-26.

[6] Y. Kortekaas, M. Dijkslag, M. Kahraman, and S. Witt. Economics of cyber security assignment block 2. https://github.com/kahraman11/EOS2019/blob/master/Block%202/report/Economics_of_Cyber_Security_Final.pdf, September 2019. Accessed: 2019-09-26.

[7] D. McGuinness. How a cyber attack transformed estonia. https://www.bbc.com/news/39655415, Apr 2017. Accessed: 2019-09-29.

[8] P. Roberts. Ddos as a cover for data theft. https://digitalguardian.com/blog/ddos-cover-data-theft, Sep 2015. Accessed: 2019-09-29.

[9] SIRE. Veelgestelde vragen. https://sire.nl/veelgestelde-vragen. Accessed: 2019-09-30.

[10] N. Woolf. Ddos attack that disrupted internet was largest of its kind in history, experts say. https://www.theguardian.com/technology/2016/oct/26/ddos-attack-dyn-mirai-botnet, Oct 2016. Accessed: 2019-09-29.