Assignment 2 - Economics of cyber security

An analysis of the darknet market The Real Deal

Group 6
Vishan Baldew - 4180992
Martijn Cligge - 4152220
Stephan Kool - 4151895
Christian Veenman - 4495705

-Last to do

- **-5b, nog in zijn geheel**
- **-4, meer uitleg actoren**
- **-6b, discussion**
- **-figure numbers**
- **-literatuur checken en op alfabet zetten**
- **-laatste keer doorlezen**
- **-Conclusion?**

1) ***Who is the problem owner of the security issue as measured in your first assignment?***

In the previous assignment, several parties are discussed that are involved with crypto markets that sell cybercrime assets. With the specific focus of cybercrime assets, such as zero-day exploits, source code and accounts, the perspective of the software company whose software is exploited is interesting to take a look at. Figure 1 provides an overview of the objectives of such a company, modeled as an 'objective tree' (De haan et al., 2009).

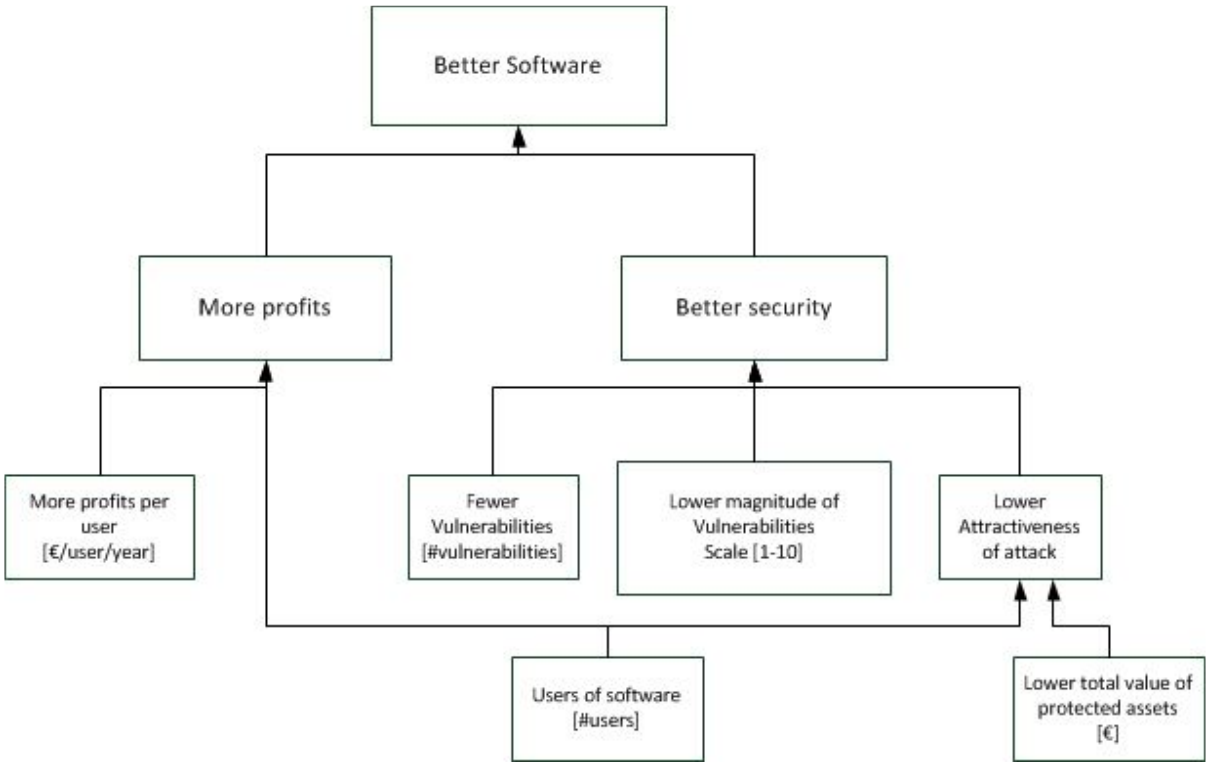

Figure 1: Objective tree software company.

This objective tree is mainly focused on the security objectives and economical objectives of the software company. Nowadays, security forms an important objective for software companies, as can be seen in the mission statement of software company Microsoft (Microsoft, 2016). However, this objective has been added later, since most companies used to have the a different mentality. This will be elaborated on later in this assignment. The security focused objective tree provide the following measurements for a software company: more profits per user, fewer vulnerabilities, lower magnitude of vulnerabilities, lower total value of protected assets and a trade off between both more and fewer users. The more users the company has, the more profits it will make (generally speaking). Yet having a high number of users also increases the attractiveness of an attack, lowering security.

2) ***What relevant differences in security performance does your metric reveal?***

Several measurements can be inferred from the dataset that is used for these assignments; a web scrape of products sold on darknet market The Real Deal. For a software company, this data is interesting for various purposes. It can for example be interesting to see how many cybercrime assets are for sale that target the company's software, and how this compares to other companies. A graph that is helpful for this can be seen in figure 2.

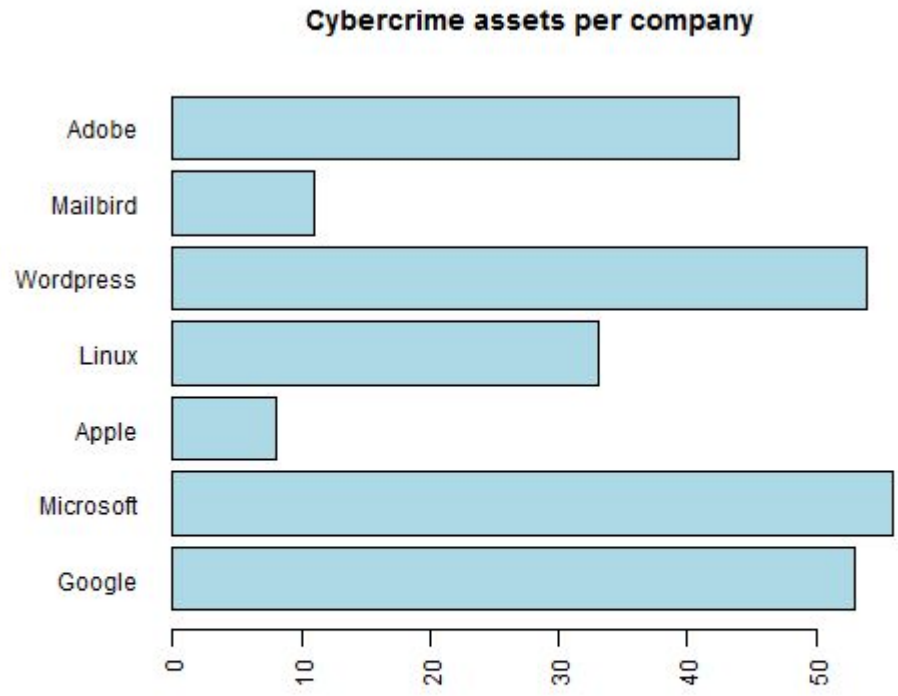

Figure 1: Cybercrime assets per software company

Even though this data seems useful at first, it turns out to be difficult to draw conclusions from this. It is difficult to compare two companies based on the number of cybercrime assets available in the market, e.g. because the companies provide different services, and have a different market share. Thus, comparing companies in this way does not provide useful information, therefore other measurements from the data are taken into account.

Another measurement that can be inferred from the data and provides much more information is the availability of various cybercrime assets, such as exploits and spam. Comparing this is interesting, because this allows for identification of possible risks for the users of the company's software. If a cybercrime asset is bought and used for a cybercrime (for example a zero-day exploit), a risk fires on the users of the software. This fired risk might lead to harm for the software users. They might accept a certain level of harm or loss, but if the harm or loss is too high they might switch to another software company (See the declining usage of Flash. One of the reasons was its security issues[1]). This will harm the sub objective *More profit* (since the number *Users of software* then goes down) of the software company (see figure 1). To identify which cybercrime assets form the biggest risk, the software company can use the measurements of amount of cybercrime assets being supplied on the darknet market.

[1]https://www.fastcompany.com/3049920/tech-forecast/the-agonizingly-slow-decline-of-adobe-flash-player

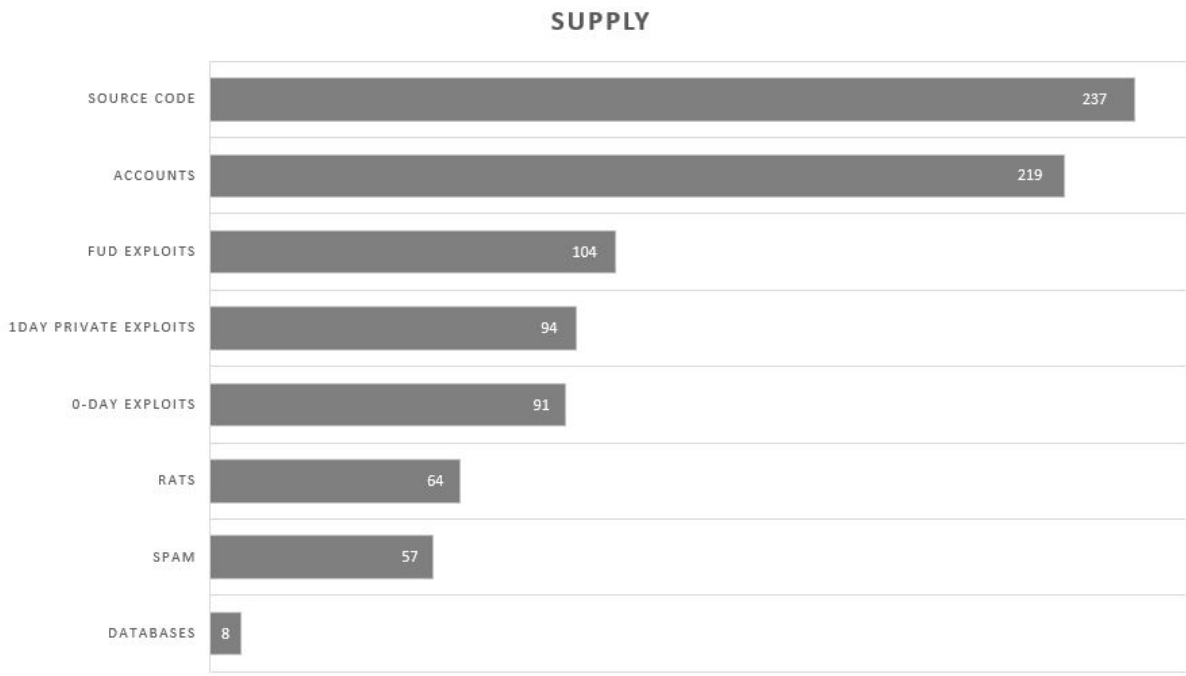

Figure 3: Supply of supply of cybercrime assets.

Figure 3 provides an overview of the various cybercrime assets that are available in the dataset. From this figure can be inferred that for some cybercrime assets there is more supply than others. According to the fair framework by Jones (2005), one can determine the risk level using the *Loss Event Frequency* and the *Probable Loss Magnitude* (see figure 3). For this assignment the supply, as displayed in figure 3, will be used as a proxy for the frequency. This means that a higher supply of cybercrime assets results in a higher frequency of loss events, because it is assumed that in order to determine a strategy only relative differences are necessary, not absolute differences.

Figure 4 FAIR framework (Jones, 2005).

The *Loss magnitude* cannot be inferred from the data either, therefore external data needs to be used to determine the impact of the cybercrime assets. The Probable Loss Magnitude for a software company is defined as *the amount of money the company loses, due to users abandoning the software company's products when vulnerabilities are exploited.* Thus, the total loss (in dollars) that the software company experiences as a result of a vulnerability, determines the probable loss magnitude, see figure 4.

There is some data available of the costs of different type of cybercrimes, for example in the report of the Ponemon Institute (2015). However, these type of cybercrime attacks are very specific type of attacks (like DOS-attacks). The dataset that is being used for this assignment, does not provide these detailed type of attacks, only broad categories of products like *Accounts*, *source code* and *zero-day exploits*. Therefore, It is very difficult to determine the exact loss that results from one user abandoning the company. This is not a major issue, since Sonnenreich, Albanese & Stout (2006:47) state that it is not necessary to quantify these losses with absolute values: *"Repeatable and consistent metrics can be extremely valuable – even if they're inaccurate"*. Therefore, a semi-quantitative LMH-scale will be used to estimate the loss.

Magnitude	Range Low End	Range High End
Severe (SV)	$10,000,000	--
High (H)	$1,000,000	$9,999,999
Significant (Sg)	$100,000	$999,999
Moderate (M)	$10,000	$99,999
Low (L)	$1,000	$9,999
Very Low (VL)	$0	$999

Figure 5 Determining PLM - FAIR framework (Jones, 2005)

For the scope of this assignment four cybercrime assets will be discussed; Spam, Accounts, zero-day exploits and RATs. Figure 6 is used to determine the risk that users will abandon software products due to certain cyber attacks.

- Spam:
  - Frequency: low
  - Impact of loss: *very low*, because it is expected that, in general, the total loss related to the amount of users abandoning the company due to e.g. one spam email is not higher than $999.
  - Risk: low
- Accounts
  - Frequency: very high
  - Impact of loss: *moderate*, because it is expected that due to e.g. lost account credentials more users will abandon the company, which results in a higher loss.
  - Risk: high
- Zero-day exploits
  - Frequency: high
  - Impact of loss: *high*, because it is expected that the total loss related to the amount of users abandoning the company due to e.g. data breaches or loss of personal information can be millions of dollars.
  - Risk: critical

- RATS
    - Frequency: low
    - Impact of loss: *high*, because it is expected that the total loss related to the amount of users abandoning the company due to e.g. others accessing their devices can millions of dollars.
    - Risk: high

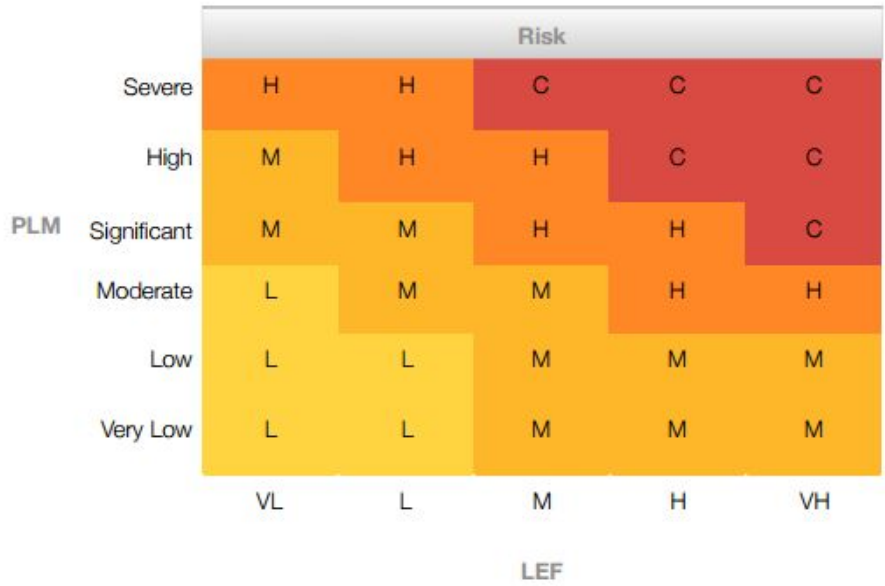

Figure 6 Determining Risk - FAIR framework (Jones, 2005).

This analysis shows the differences in security performance for different cybercrime assets. The software company can use these differences to determine which cybercrime assets might form the biggest threat. It might be wise to adopt certain risk strategies to reduce the impact or mitigate the loss event frequency. It should pay in particular pay attention to zero-day exploits. This will be elaborated on later.

3) What risk strategies can the problem owner follow to reduce the security issue as measured in your first assignment?

The analysis of question 2 showed that zero-day exploits form the biggest threat to software companies. The problem of the availability of the cyber security exploits on the crypto markets creates essentially a principal-agent problem. The victim of zero days is generally not the vendor of the software to which the zero day belongs, but the user of the software (Ingols, K et al. 2009). The vendor do has an interest in keeping its software safe from the cybercrime sold on the crypto markets because doing nothing could lead to a bad reputation at best, and the loss of all clients at worse. The asset at risk for the software company that produces the service or software targeted by the cybercrime products are the clients that use the software or service. Therefore the problem owner can accept, reduce, transfer or avoid the risk of losing users (Khakzad et al. 2012) Accepting the risk means taking the risk for the user of the software without applying any risk-reducing measures.If things go wrong, it is up to the software company to pay for all of the damages caused. Avoiding the risk is the other extreme: this would make the company stop the activity of the product or service altogether that is affected by a risk. Transferring risk means that someone else is made responsible for

the risk that occurs. And finally risk-reducing techniques are divided into three options: detection, control and mitigation measures (Neil, N. F. and M., 2012).

The cyber attacks defined in the previous section serve as the risk threats that require the accept, reduce, transfer or avoid strategies.

Spam

Spam is directed of the users of email addresses and a software company in this specific case is a provider of webmail services such as Yahoo or Google mail or a corporate provider of an email server such as the Microsoft Exchange servers. It is assumed that if the software company leaves through too many spam emails, there is an unknown likelihood that a user of the service will switch to a different provider.

The company can accept this risk and let all emails go through. Avoiding the risk would mean stopping the service altogether. To transfer the risk, the software company could get an insurance for lost clients because of spam or could agree in a contract that the client is responsible for the spam. Finally, the company could implement a spam filer or provide awareness courses and campaigns for spam, as depicted in figure 7 below.

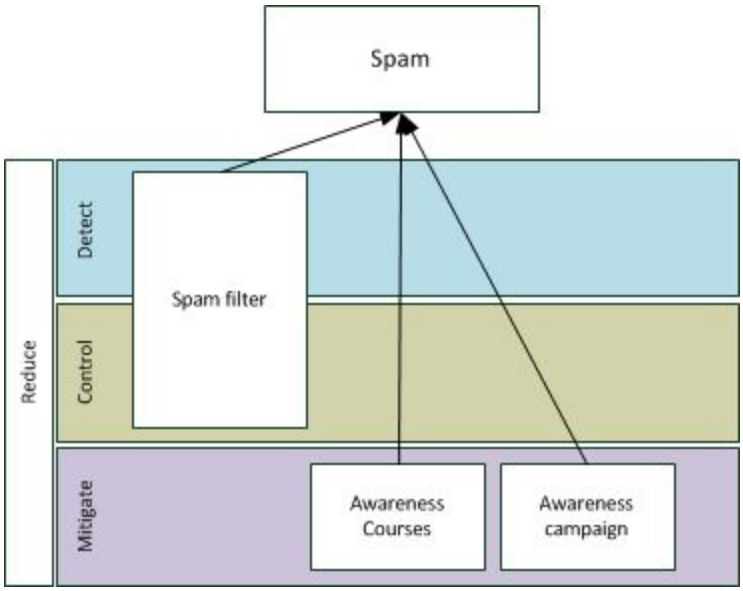

Figure 7: Spam threat reduction means

Accounts

With the accounts being out there already is generally the result of a hack. Accepting the risk of losing clients means doing nothing and letting it all play out. Reducing means that the company whose client data has been stolen should, in order to keep the trust of the customer, proactive in the disclosure of the information of the breach and the spread of the data, which requires an intrusion detection system or similar. Also, to reduce the impact of the breach the client data should be hashed as much as possible. Transferring risk could take place in form of an insurance against data breaches and avoiding is stopping the service that contained the client data before the breach happened.

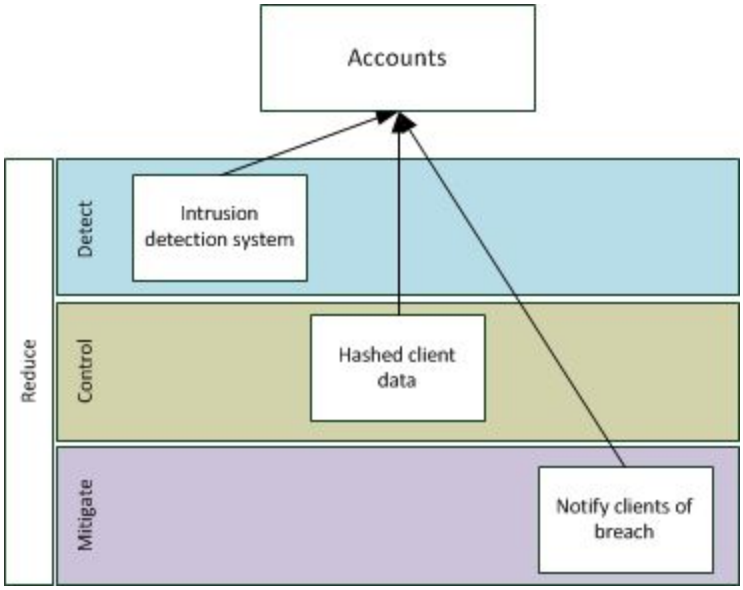

Figure 8: Accounts threat reduction means

Zero-day exploits

zero-day exploits can by their nature not actively be prevented. Accepting the risk of a zero day causing users to stop using the software means that nothing is undertaken to reduce the risk, but also no additional costs are made. Risk reduction in more on the detection and mitigation side, as in quickly discovering the usage of zero-day exploits and then having a quick patching system present. A second form of risk reduction is offering bug bounty program in which zero-days and other exploits are bought by the company at prices close to the crypto-market levels and as such providing a viable alternative to illegal trade and business models based on exploits discovery. A single Windows exploit listed at around $90.000 could get between $50.000 and $100.000 though the bug bounty program (Krebs B., 2016) Transferring this risk may be possible through insurance, if there is an insurance company willing to take the risk. Avoiding also means closing the business activity linked to the software in which the zero day has been found.

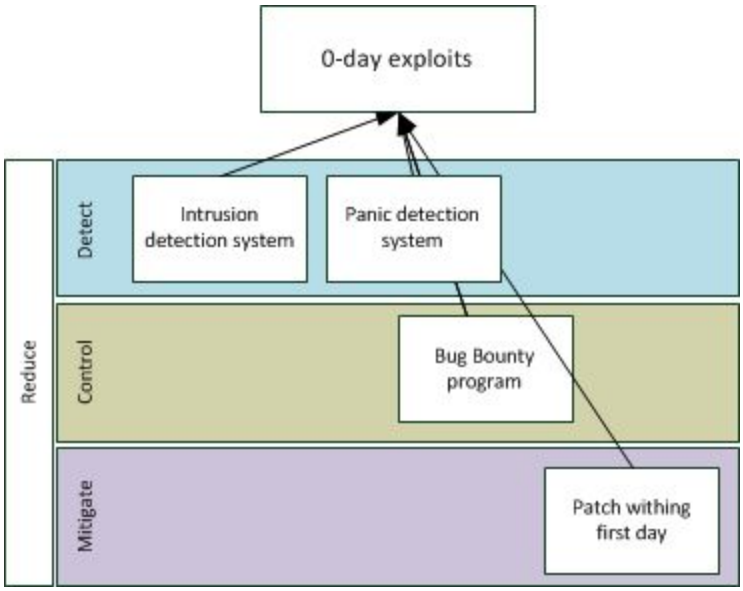

Figure 9: Accounts threat reduction means

RATs

Finally, Remote Access Tools allow for accessing and controlling a distance computer, generally through an already know but yet unpatched weakness in the target's software. Accepting the risk means that such an exploit may lead to loss of users. Reducing the risk, as shown in the figure 10 below could include IDS, forced updates and making customers aware of the dangers of outdated software. The transfer of the risk could be an insurance against the loss of income through lost clients, or explicitly stating that updating software is the responsibility of the customer or user. Finally, there is always the option to avoid the risk by stopping the business activity.

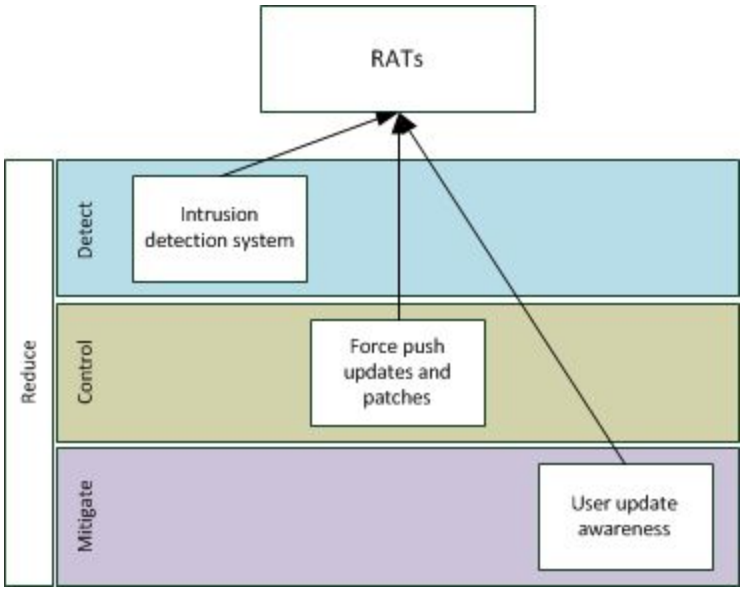

Figure 10: Accounts threat reduction means

4) ***What other actors can influence the security issue as measured in your first assignment?***

As discussed in our previous assignment, there are different policy decision makers that are able to affect the security issue. To be specific, apart from the problem owner, both the police task force and the crypto market operator have the ability to influence the existence of the crypto market - which is synonymous with the high availability of the cybercrime exploits. The crypto market is the asset of the crypto market operator. As such, the operator will be the one taking defensive measures for the protection of the market, as well as his own identity since the activities are illegal. The operator facilitates the trades between buyer and seller by operating the platform that allows for the exchanges. The police task unit is charged with reducing the free availability and is therefore set to attack the asset of the crypto market operator, the crypto market. The police task unit does not have a well defined asset at risk and as such will assume the role of attacker, whilst the crypto market operator will defend.

The buyers and sellers on the crypto market do influence the security issue, but to a much lower degree that the crypto market operator and the police task force. Although sellers make the cybercrime tools available, only the market itself creates the actual availability for potential buyers. The buyers also contribute by creating a market for cybercrime tools, incentivizing both the sellers and the operators to continue their work. However, both the sellers and the buyers are not actual security decision makers that, through their security decisions, influence the availability of the crypto market.

However, result of the trade on the crypto market is the free availability of cybercrime tools, which target the software created by a software company and and as such harm the assets of the software user. This creates a principle-agent relationship between the software company and the software user as the software company claims (partial) ownership over the software that is exploitable and the software user is the victim of such an exploit. However, the user may have a dependency on the software based on the case and the software company has a dependency on the user for income.The formal chart (figure 11 below) explicits the relation between the different actors.

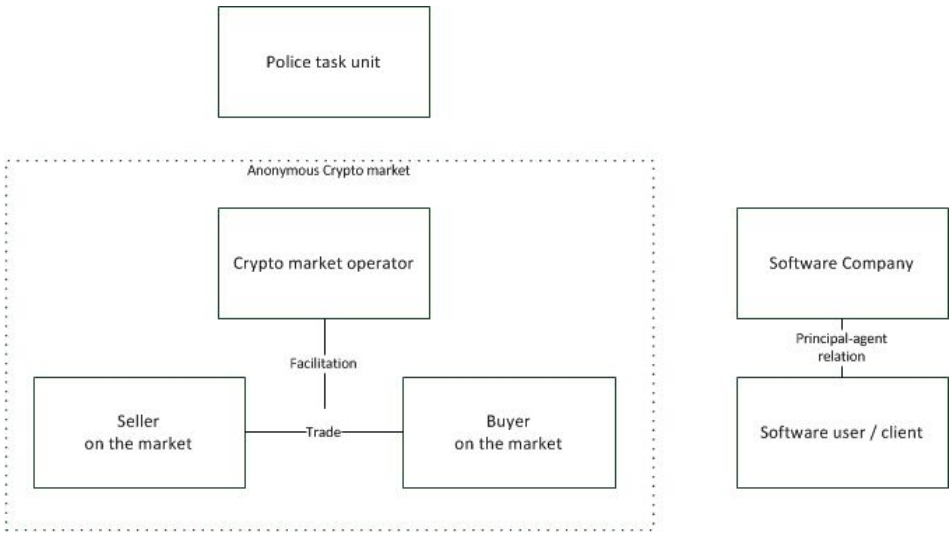

Figure 11: Formal chart actor relations

5) ***Identify the risk strategies that the actors can adopt to tackle the problem***
a) are there actors with different strategies? why?

Crypto market operator

The crypto market operator's main asset is the crypto market safety and his own.
Police forces will actively pursue the crypto market operator and try to identify his identity as well as gaining access to the market platform itself. This creates three risk abstractions for the market operator: having a police mole in the platform though a compromised buyer or seller, having its own identity uncovered and losing access to the crypto market. As with all the above cases, the operator can simply accept the risk. However, this will most likely lead to the loss of the market and lead to a conviction for the operator. Transferring risk is very difficult, it is doubtful there is an insurance company willing to take up the risk for the operator. Avoiding the risks means shutting down the market. The risk reductions are modeled in the diagram below:

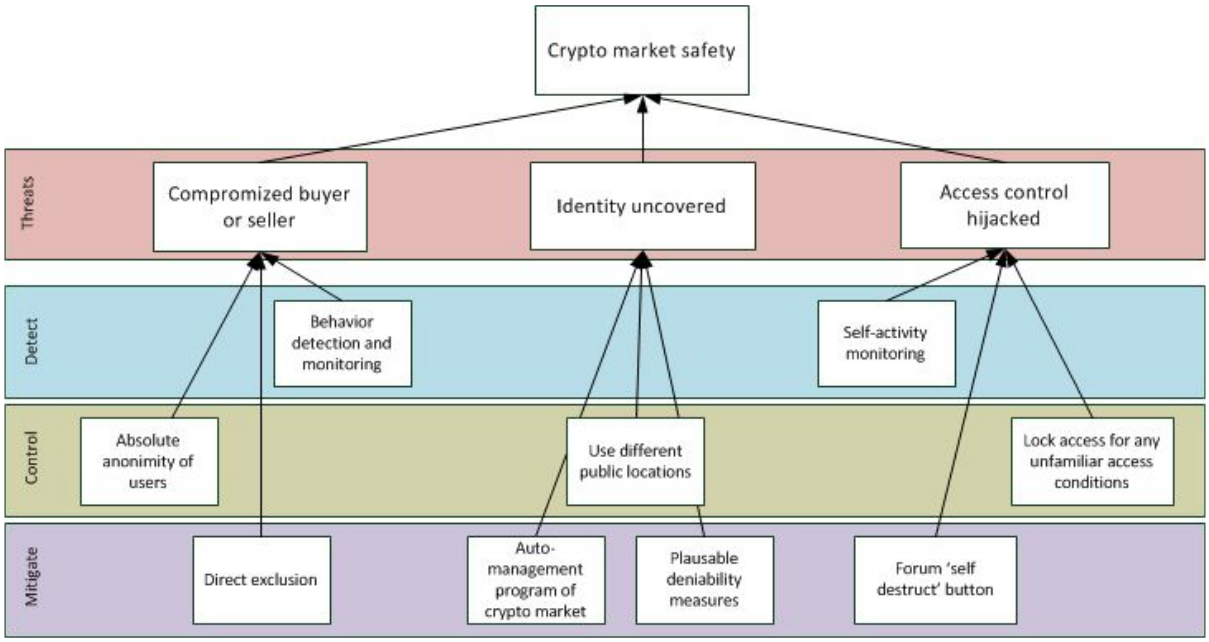

Figure 12: Means-Threat diagram crypto market operator

Police task force

If the crypto market operator is the defender of the crypto market asset, the police task force is the attacker. With the objective of reducing the illegal trade that goes through the crypto markets, the police task force has three possible points of attack: the sellers and buyers, the crypto market operators or the crypto market service environment. This is in line with the defence strategies for the crypto market operator.

Since the police task force takes up an attacking role and does not have an asset that requires defending, it makes little sense to model the means of the police task force in risk categories of acceptance, reduction, transfer and avoidance or the specification of reduction into detection, control and mitigation. Therefore, the result is a more classical means-end diagram as depicted in the figure 13 below.

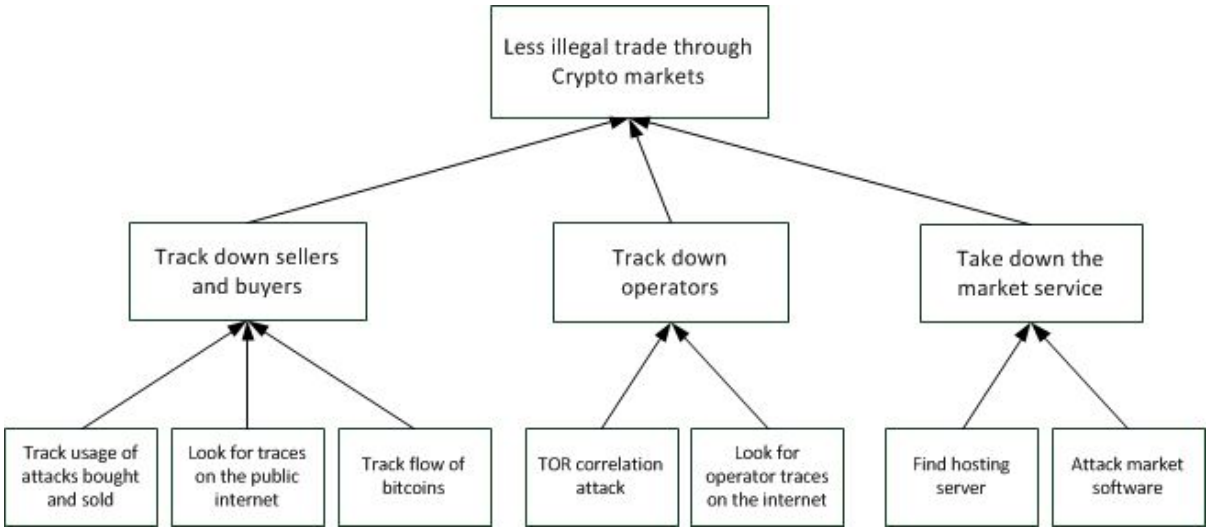

Figure 13: Means-End diagram Police Task Force

The means of the police task force are as follows:

- Track usage of attacks which are bought and sold on the markets
- Look for any traces on the public internet that match with the traces of the buyers and sellers on the crypto market
- Track the flow of bitcoins
- Perform a TOR correlation attack
- Look for traces of the operator on the public web
- Find the server hosting the service and take it down
- Attack the software on the platform

b) have the strategies changed significantly over time in a way that reduces or increases risks?

For specific software companies, there has been a notable change of strategy. A prominent case is Microsoft with the operating system Windows, which in its monopolistic market position could get away with delivering an operating system that was unstable and not very secure. Microsoft was known for shipping first and fixing it at a later version (Boehm, 2016). Nowadays, Microsoft has competition on the desktop operating system market from apple, and can no longer afford to ship faulty software. The risk of losing a client has become larger because the viable alternative to which to switch to exists. As such, Microsoft moved more away from a full risk transfer to the user of the software to taking some responsibility and implementing more control and detection measures, such as shipping Windows with a firewall by default.

However, there is also a different direction that software providers can go. The Valve Steam Store has a section for independent video game makers to sell their games to a large public. In general, these independent developers opt for a so called 'early access' option in the sales, where the game is sold at a reduced price but unfinished, lacking content, with many bugs and the promise of improvement. Though the early access sales, many risks are transferred to the user of the software but the user can be considered to be informed of this and having the financial benefit of paying less.

6) Pick one of the risk strategies identified previously and calculate the Return on Security Investment (ROSI) for that particular strategy. I.e.,

For this analysis the Return on Security Investment (ROSI) will be calculated to analyze if it is interesting for the problem owner to invest in a certain risk strategy. ROSI is a well-known method to calculate the return (profit) that a security investment can generate by covering part of the impact or probability that would otherwise have been taken.

Return on Security Investment (ROSI) can be calculated with the following formula:

$$Return\ on\ Investment\ = \frac{(Risk\ Exposure * Risk\ Mitigation) - Solution\ Costs}{Solution\ Costs}$$

For the analysis of the ROSI, a risk strategy is analyzed that aims to reduce one of the highest risks for a software company. The analysis of the metric for the supply of the different type of cybercrime assets in question 2 of this assignment showed that zero-day exploits might form the highest risk for users. If a risk fires, users might abandon the software of the software company. Therefore, it is interesting to analyze the ROSI of a particular risk strategy that aims to reduce the risk of zero-day exploits. Since most numbers used in this analysis are estimates, a range estimation with a minimum and a maximum value is used instead of a point estimation with a uniform linear distribution.

a) Estimate the costs involved in following that strategy

The solution costs are the costs associated by implementing a security solution (Sonnenreich, 2006). This does not limit itself to just the system or software itself, but it also includes an increase and decrease in productivity, the costs related to applying the solution to your company, etc. The unknown - and hard to predict - indirect costs make it is very difficult to come up with numbers for the costs of cyber risk solutions (Boehm, 2016) .

The strategy of the risk strategy consist of the following means: the intrusion detection system, panic detection system, bug bounty plan and the patching system. For this analysis, the ROSI for the patching system and the buy-off plan will be analyzed. On the website of Zerodium (2016) various price plans for buy-offs are found. The solution costs for the buy-off plan is differs per platform. Prices for zero-day exploits for e.g. Apple are much higher, probably the supply of those zero-day exploits is lower, which might mean that the software is safer. This is also what our metric showed in question 2 of this assignment. In addition to this, Microsoft told researchers of Trustwave in an interview that it pays between 10.000-50.000 dollar per zero-day exploit (Krebs, 2016). So, the average price of these bounty prices is taken as the solution cost for that particular strategy. This would be around 30.000 dollar. Patching is another mean which a software company can use to deal with zero-day exploits. In a report of Telang and Wattal, S. (2007), it is stated that the average patching cost for Microsoft is around 100.000 dollar. This results in a combined cost of **130.000 dollar.**

b) Estimate the benefits of following that strategy.

Now that the solutions costs are determined, the risk exposure and risk mitigation need to be determined to be able to calculate the ROSI.

Risk Exposure

The risk exposure is the amount of damage to a certain asset when a vulnerability is exploited by a threat because control measurements are not in place or do not work effectively. The risk exposure is often hard to calculate or define because of the inability to accurately predict when threats will exploit a vulnerability and what the damage of such an exploit is. One reason for this is that companies who had an attack often do not want to tell the exact damage, since this might have a negative impact on their reputation. The risk exposure of an zero-day exploit really depends on who the actual victim of the attack is and what the asset is that is being attacked. The risk exposure in the ROSI formula consists of two parts, the single loss exposure and the annual rate of occurrence:

$$Risk\ exposure = Single\ Loss\ Exposure * Annual\ rate\ of\ occurrence$$

Single loss exposure

There is no information about the damage of a single zero-day exploit, since zero-day exploits can be used for various criminal activities, like espionage or data theft. Therefore, for this analysis the average loss per year of all cybercrime attacks for a single company is taken as the loss. This number is around 11.5 million dollars (Hardekopf, 2015). This includes all type of attacks, so this number might be to high as the single loss exposure for a single zero-day exploit. Therefore a slightly lower number with a range estimation of **9-13 million dollar per year** is taken for this analysis. This is already the total risk exposure, since this is calculated per year. Therefore it is not necessary to determine the single loss exposure of a single zero-day exploit.

Annual rate of occurrence and updated solution costs

There is some information about certain organizations that analyzed the number of zero-day exploits in the year 2015 on the website of fire-eye (2015). This information can be used to get some impression of the number of used zero-day exploits per year. In the year 2015, 13 zero-day exploits were detected. To calculate the new solution cost, the number of 2015 is used. The new solution costs are now equal to the average amount of zero-day exploits per year times the cost for one zero-day exploit, 13 * 130.000 = **1.690.000 dollar.**

Risk Mitigation

Risk Mitigation is expressed as a percentage and represents the amount of damage that is avoided when the investment in place. Again, it is very difficult to determine the exact mitigation effects of patching and the bounty plan, because only the known vulnerabilities are known, the amount of unknown vulnerabilities that can be used for zero-day exploits is of course unknown. The book “Cyber-Risk Informatics: Engineering Evaluation with Data Science” estimates this to be between **25% and 50%** depending on the solution. Since there is very little information about the effectiveness of patching and the bounty programs, these numbers are used to determine the ROSI.

ROSI applied

The analysis provided the following numbers for calculating the ROSI:

- Solution costs: $1.690.000 per year.

- Risk exposure: $9.000.000 - $13.000.000 per year.
- Risk mitigation: 25% - 50%

$$Return\ on\ Investment_{E=9m,\ M=25\%} = \frac{(9.000.000 * 25\%) - 1.690.000}{1.690.000} = 33,1\%$$

$$Return\ on\ Investment_{E=13m,\ M=25\%} = \frac{(13.000.000 * 25\%) - 1.690.000}{1.690.000} = 80,0\%$$

$$Return\ on\ Investment_{E=9m,\ M=50\%} = \frac{(9.000.000 * 50\%) - 1.690.000}{1.690.000} = 166,25\%$$

$$Return\ on\ Investment_{E=13m,\ M=50\%} = \frac{(13.000.000 * 50\%) - 1.690.000}{1.690.000} = 284,6\%$$

Is it worth it?

Depending on the risk exposure and the actual risk mitigation percentage, the ROSI varies. The results, however, are all indicating a positive ROSI; even the ‘worst case’, where the risk exposure is $9 million and the amount of attacks mitigated is 25% percent, the solution still has a return of 33,1% of its investment costs. This might be the case where the estimated damages due to zero day attacks have been rather overestimated, and the resulting amount of exploits have been rather underestimated. This results in a less higher ROSI because the solution prevents less damage than initially thought. In the ‘best case’ with a risk exposure of $13 million and 50% mitigation of all the attacks, the ROSI is relatively high, with a return of 284% of the investment cost of the solution. Even though the risk exposure and mitigation are varying, it might be a good investment to spend money on the solution - of course under the circumstances that the estimated range holds. Whenever the estimated risk exposure is too low, it becomes possible that the costs of the solution are higher than the benefits - the ROSI can then become negative. However, in the situation as described above, this situation is not very likely to occur.

References

Boehm (2016) Lecture cyber risk strategies.

De Haan, A., W. P. A. C. Willemse, P. de Heer, S. C. Vos, and P. W. G. Bots. "Inleiding technische bestuurskunde."

Fire-eye (2016) Recent zero-day exploits. Retrieved on 13-10-2016 from https://www.fireeye.com/current-threats/recent-zero-day-attacks.html(2009).

Bill Hardekopf (2015) An "Average" Cyber Crime Costs a U.S. Company $15.4 Million. Retrieved on 13-10-2016 from: http://www.forbes.com/sites/moneybuilder/2015/10/17/an-average-cyber-crime-costs-a-u-s-company-15-4-million/#7027fe911a22

Ingols, K., Chu, M., Lippmann, R., Webster, S., & Boyer, S. (2009). Modeling modern network attacks and countermeasures using attack graphs. Proceedings - Annual

Computer Security Applications Conference, ACSAC, 117–126. http://doi.org/10.1109/ACSAC.2009.21

Jones, J. (2005). An Introduction to Factor Analysis of Information Risk (FAIR). Risk Management Insight.

Khakzad, Nima, Faisal Khan, and Paul Amyotte. "Dynamic risk analysis using bow-tie approach." *Reliability Engineering & System Safety* 104 (2012): 36-44.

Krebs B, (2016, May 16). Got $90,000? A Windows 0-Day Could Be Yours. Blog post, retrieved on 16-10-2016 from https://krebsonsecurity.com/2016/05/got-90000-a-windows-0-day-could-be-yours/

Mehmet Sahinoglu (2016) “Cyber-Risk Informatics: Engineering Evaluation with Data Science”

Microsoft (2016) What we value. Retrieved at 13-10-2016 from https://www.microsoft.com/en-us/about/values
e

Neil, N. F. and M. (2012). The Need for Causal, Explanatory Models in Risk Assessment 2.1, 31–50. Ponemon Institute L (2015) Cost of Cyber Crime Study: Global.

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.

Telang, R., & Wattal, S. (2007). An empirical analysis of the impact of software vulnerability announcements on firm stock price. IEEE Transactions on Software Engineering, 33(8), 544-557.

Zerodium (2016) Our Exploit Acquisition Program. Retrieved on 13-10-2016 from https://www.zerodium.com/program.html