Assignment Block 3

SPAMHaus

DRAFT

Group 8
Jorrit van den Spek, Hugo Bijmans, Eveline Pothoven, Ben Hup, Lisette Altena

WM0824 Economics of Security

Table of Contents

1. Introduction

To be written

2. Who is the problem owner of the security issue as measured in your first assignment?

The security issue chosen in our first assignment is phishing. Phishing is a kind of internet fraud where criminals attempt to obtain sensitive information like usernames, passwords or credit cards details (Alert Online, 2016). Phishing attacks tend to use spamming services, like spamming botnets, a lot. A fake bank website is made and a botnet is rented to send a SPAM message to vulnerable people. Even tough spamming is mostly an end-user problem, the problem owner chosen for this assignment is the Government of the attacked country. To reduce that scope even more, we will mainly focus on the Department of Economic Affairs. So in the Netherlands, this will be the "Ministerie van Economische Zaken". But since the Netherlands isn't massively attacked by phishing/ spamming attacks in comparison to the United-States, the focus will be on the Department of Economic Affairs of the United States of America (Kaspersky, 2016).

The goal of the Department of Economic Affairs is to support and improve economic activity as much as possible. This organization works to create jobs and expand economic opportunities everywhere they can (State.gov, 2016). It does so by negotiating with various parties all over the world to ensure the economic growth of the United States remains high. Everything that can threaten this position is threatening the goal of the Department of Economic Affairs, so this actor will do whatever it's able to do to prevent that.

Since our security issue is phishing, the main risk for the Department of Economic Affairs is to lose economic momentum, productivity of even real money due to phishing. Economic damage can be caused by simply the time spilled by employees on deleting or answering phishing mails, malware infections after a phishing attack or money stolen by fake bank website. So the Department of Economic Affairs has serious incentives to stop phishing from happening. The strategies it has to accomplish that are discussed in the next sections of this report.

3. What relevant differences in security performance does your metric reveal?

Due to personal reasons, this part is missing, but will be present at the feedback session on Thursday.

4. Risk strategies

Risk strategies can be followed by the problem owner to reduce a security issue. Risk strategies are part of a broader risk management plan as defined in ISO 27001 (ISO.org, 2016). Broadly, there are four potential strategies that can be used to handle risk:

1. Avoid risk – circumventing risk; for example by ceasing activities altogether
2. Mitigate risk – Reducing the impact or likelihood (or both) of risk
3. Accept risk – accepting negative (or positive) impact of a risk
4. Transfer risk – outsourcing risk to a third party or parties that manage the risk for you

In the context of the SPAMhaus dataset and the three actors (i.e. government, cyber security companies (CSCs) and Internet Service Providers (ISPs)) the potential strategies can be defined as follows:

1. Avoiding risk means:
    a. Government – cutting citizens from the Internet or at least firewalling the country from access to other nations (e.g. like the great firewall of China). Another less rigorous intervention would be only blocking all e-mail related protocols (e.g. POP3, IMAP and SMTP)
    b. CSCs – can advise their clients to stop using e-mail
    c. ISPs – have the technical expertise and blocking power to in fact block all e-mail related protocols from all devices in a certain country
2. Mitigating risk:
    a. Government – Informing citizens, own governmental departments and the private sector about SPAM and creating awareness of potential threats that can materialize in an impact with certain behaviour of these actors. Furthermore, the government has more stringent and permanent options to consider as the *trias politica* divides jurisdiction in three segments. First, the *legislative branch* is able to create new laws to defend against SPAM. Second, the *executive branch* is able to execute laws that have been passed (e.g. police officers). Third and finally, the *judicial branch* applies laws and convicts individuals and organizations when the law is broken.
    b. CSCs – have (tacit) knowledge to inform companies and other organizations to consult, create awareness and give practical advice how to mitigate cyber risk.
    c. ISPs – can mitigate risk by educating their support staff on SPAM and botnets. Support staff will be better able to detect and give assistance to out of the ordinary computer behaviour when clients describe it (e.g. slower computer phishing, and slow Internet connection). ISPs can also execute a law passed by the *legislative branch* of government, for example to block SPAM or pre-emptively scan e-mails for viruses, malware and worms.
3. Accept risk:
    a. Government – can accept the risk by just letting SPAM happen and leaving citizens and organizations to self-organize
    b. CSCs – can also accept SPAM risk and focus on other forms of risk that might have a higher impact
    c. ISPs – can accept the SPAM risk by leaving customers at their self-organizing power

4. Transfer risk:
    a. Government – could enact a law for customers to share the risk of (im)material damage to customers. This way customers might collectively help each other as shared knowledge about SPAM and its risk directly influences the premium each customer has to pay for the 'SPAM insurance'.
    b. CSCs – could advise customers on a safer cyber environment and might offer insurance against risk at the principle that a customer must install a minimum amount of security to mitigate risk and if risk nevertheless materialises then is covered by insurance.
    c. ISPs – could also offer customers insurance with the rule that a customer must install a minimum amount of security to be applicable to receive insurance. When a risk materialises in an impact the customer will be covered for damages.

5. Other actors influencing security issue

In the previous and this report are defined three actors: government, Cyber Security Companies (CSCs) and internet Service Providers (ISPs). There are many other actors influencing the SPAM security issue. The most important identified for this report are:

1. Botnet masters – are the shepherds of a botnet and access bots via *Command and Control nodes* (C&C's). Bots will not send SPAM or do anything without an explicit instruction given by a C&C. Destroying the C&C's immobilizes the shepherds flock. Closing C&C's is effectively a root-cause solution by both stopping the SPAM and stopping control over botnets.
2. Consumers – are individuals and households that connect to the Internet for information and all kinds of offered services. Consumers are one of the most important actors influencing SPAM security risk. Awareness of consumers means that they could change their behaviour to prevent falling victim to SPAM related accidents. If less consumers click on the links embedded in SPAM, then operating a C&C will not be profitable and thus a Botnet Master will seek his income from other criminal activities.
3. Businesses – are connected to the Internet to create value for customers. Besides consumers also businesses and it personnel can be made aware of SPAM impact and security policies. Moreover businesses should focus on the security of e-mail servers and devices besides merely focussing on whether an application is working.
4. Money mules – are the actors that withdraw money stolen from consumers. C&C's deposit stolen money in a real bank account. Money mules are random anonymous people that go to an ATM and withdraw the money while withholding a percentage for their service. The money is dropped off at a certain physical location and gathered by the botnet masters. Stopping the recruitment of money mules by botnet masters would be a near root-cause solution as the money does not reach the botnet masters. In addition, Botnet masters do not want to withdraw the money from a bank account themselves in order to stay anonymous.
5. Programmers (malware code writers) – are the actual creators of C&C's and write the code to infect new devices that, after infection, are added as a bot to a botnet. Stopping botnet code writers from writing botnet related code would also be a root-cause solution. However, this is nearly impossible as every human being has the fundamental right to have privacy at home. Moreover, a malicious person can write the botnet code in the privacy of his home where the privacy is protected by law.

Some actors like botnet masters and botnet programmers play a primary role in the activation and maintenance of a botnet that sends SPAM. Furthermore, money mules are located close to the root-cause of the SPAM problem as they withdraw the stolen money from malicious phishing SPAM and physically bring it to the botnet masters. Consumers and businesses also play their part in the SPAM security issue as they are responsible for clicking on links in (phishing) e-mails and leaving their guard down and not creating and enacting security policies so new botnet infections may occur.

6. Identify the risk strategies that the actors can adopt to tackle the problem

In this section the risk strategies of the actors described in the previous section will be discussed. These actors are the botnet masters, the consumers, businesses, money mules and the malware programmers. The sociotechnical nature of the system ensures that these actors have different and even conflicting strategies. These conflicting strategies will be pointed out and the change of these strategies throughout will be given.

The botnet masters control the botnet via C&C. It is the only way for them to communicate with the bots. It is essential that the C&C is protected because without it the botnet masters can't reach their network and thus make money. To reduce the risk the botnet master should use a way to communicate to the bots via the C&C that anti-virus/malware software will not detect. One popular C&C communications technique is to use publicly available DNS servers rather than the systems inside a private network. Advanced-persistent-threat actors try to use public DNS services to avoid logging within the private network and risk detection. (James Ringold, 2014) The goal to protect the C&C servers is the direct opposite of what the problem owners, mentioned in the previous section have namely, to disrupt the C&C. The consumers and business also have conflicting strategies because they are the ones targeted.

Strategies used by consumers are listed in the category risk mitigation and risk transfer. The consumers can mitigate risk by installing firewalls, make back-ups and don't open untrustworthy emails. Consumers can also transfer the risk toward the ISP. In this case a contractual agreement of financial compensation with the ISP is formed.

Businesses are targeted a lot by SPAM, The annual cost due to loss in productivity through SPAM is estimated to be around $20 billion, based on the percentage of an employee's time spent browsing and deleting individual SPAM messages during a given day at work. (Feroze, 2015) Businesses tend to have a lot of the same risk strategies as the consumers, but cannot accept certain risks for legal reasons. To make sure privacy data of costumers and other sensitive data is not leaked, employees should be trained in recognising SPAM. A proactive strategy, such as staff training and adoption of innovative strategies in a timely fashion, can yield significant benefits at reasonable costs. (Rowe, 2006)

Money mules make the withdrawals from the bank accounts the money generated by the botnet are transferred to. The names of the botnet masters or the money mules are not registered to these bank accounts which leave them anonymous. The withdrawals are physically done at ATMs which make them irrelevant for cyber security risks strategies, but interesting for other government forces.

Malware programmers are the coders that create the C&C's and write the code that infects the machines. Malware uses various techniques to camouflage itself and to make their lifetime as long as possible. Although, camouflage approaches cannot fully stop the analysing and fighting against the malware, it makes the process of analysing and detection prolonged, so the malware can get more time to widely spread all over the net. (Rad, 2012) To reduce the risk to get their malware detected the programmers need to keep investing in new techniques to camouflage the malware.

The actors described above have clear opposite interest concerning SPAM. On the one hand there are the criminals and on the other hand there are the actors targeted by the criminals. The constant change in threats and vulnerabilities ensures that all actors have to change their risk security strategies throughout time.

7. Return on Security Investment

7.1 Costs of following the strategy

The US government announced in the Cybersecurity National Action Plan (CNAP) that over $19 billion will be invested for cybersecurity as part of the President's Fiscal Year 2017 Budget (The White House, 2015). A new campaign will start to raise public awareness of the individual's role in cybersecurity and training that helps people to spot phishing attacks and other related threats. It is estimated that one fifth of the total cyber security budget ($3.8 billion) will be used for this campaign.

A major part of the costs from phishing results from financial theft. Therefore companies in the financial sector are recommended to take steps. American Express and Visa, spend $30 million to improve the security of their systems (The White House, 2014). The total costs of following the strategy are $4.1 billion for the next year.

7.2 Benefits of following the strategy

The benefits of a strategy correspond to the expected prevented losses. The costs from a cyber event can be differentiated among first and third party losses. First party losses are the costs which are a direct result from the incident. In the case of phishing this may include the dollar value of financial theft. Third party losses relate to the costs from private legislation, or fines or fees brought by government agencies.

Table 1 shows the costs of phishing, retrieved from a research of Romanosky (2016), which investigated the costs of cyber incidents. In this research 12.000 cyber events in the United States were examined, of which in 7.3 % of the observations (or 921 instances) financial data was available.

Table.1 Costs by event type (in millions)

Event type	N	Mean	SD	Median	Min[a]	Max
Data Breach	602	5.87	35.70	0.17	0.00	572
Security Incident	36	9.17	27.02	0.33	0.00	100
Privacy Violation	234	10.14	55.41	1.34	0.00	750
Phishing	49	19.99	105.93	0.15	0.01	710
Total	921	7.84	47.28	0.25	0.00	750

[a] Values are presented in millions of dollars and therefore any zero values are artefacts of rounding functions.

These costs are incomplete however. It doesn't include lost revenue, sales and market valuation. Furthermore intangible or nonfinancial costs like lost reputation or productivity are not considered. Nevertheless, research of Ponemon Institute (2015) has shown that 48% of the total costs are caused by productivity losses.

The Ponemon Institute conducted research on the cost of cybercrime with a representative sample of 58 organizations in both the public and private sector located in the United States. The benchmark consisted of only large-sized companies (1000+ employees). The costs include all factors mentioned above.

The report shows the results for this benchmark in the "2015 Cost of Cyber Crime Study: Global" report, presented last year (Ponemon, 2015a).

- On average $15.42 million cost of cybercrime annually
- Percentage phishing of annualized cybercrime cost: 14%

This means that phishing costs a company on average $2.16 million annually. Multiplying this annual cost per (large-sized) company with the number of companies in this category (table 2), leads to a total annual loss from phishing of $32 billion. Considering that businesses have only 39.9% of the breaches (table 3), the total annual loss from phishing is $80,4 billion.

Table 2 USA business list - employee size profile (DMDatabases, n.d.)

# of employees	Quantity
10,000+	1,811
5,000-9,999	1,707
2,500-4,999	4,180
1,000-2,499	7,158
Total	**14,856**

Table 3 Five industry sectors affected by breaches in 2015 (Urrico, 2015)

.

Industry	% of breaches
Businesses	39.9
Medical/healthcare	34.8
Banking/credit/financial	9.6
Educational	8.3
Government/military	7.4

Research of security technology company Wombat showed that the training of employees could help cut the costs by 50% (Greenberg, 2015). So, the total benefits of following the strategy would be $40.2 billion.

7.3 Calculating RoSI

The return is on security investment is calculated with

$$RoSI = \frac{Risk\ Exposure \cdot \%Risk\ mitigated - cost}{cost}$$

Filing in the values determined in the previous paragraphs, gives:

$$RoSI = \frac{\$80.4B \cdot 50\% - \$4.1B}{\$4.1B}$$

$$RoSI = 8.8$$

8. Conclusion

To be written

References

Alert Online. (2016). *Phishing | Alert Online.* Website visited on 6-10-2016, via: https://www.alertonline.nl/experts/wat-is-phishing

DMDatabases. (n.d.). *USA Businesses List*. Retrieved from http://dmdatabases.com/databases/business-mailing-lists/how-many-businesses

Feroze, M. A., Baig, Z. A., & Johnstone, M. N. (2015). A Two-Tiered User Feedback-based Approach for SPAM Detection. *ICSNC 2015*, 22.

Greenberg, A. (2015). Report: *Phishing costs average organization $3.7 million per year*. Retrieved from http://www.scmagazine.com/report-phishing-costs-average-organization-37-million-per-year/article/435037/

KasperskyLab. (2016). *Securelist: SPAM and Phishing in q1 2016.* Website visited on 6-10-2016, via: https://securelist.com/analysis/quarterly-SPAM-reports/74682/SPAM-and-phishing-in-q1-2016/

ISO.org (2016). *ISO/IEC 27001 - Information security management*. Website visited on 10-10-2016, via: http://www.iso.org/iso/home/standards/management-standards/iso27001.htm

Ponemon Institute. (2015). *The Cost of Phishing and Value of Employee Training*, 16.

Ponemon Institute. (2015a). *2015 Cost of Cyber Crime Study: Global.* http://www8.hp.com/us/en/software-solutions/ponemon-cyber-security-report/index.html?jumpid=va_fwvpqe387s

Rad, B. B., Masrom, M., & Ibrahim, S. (2012). Camouflage in malware: from encryption to metamorphism. *International Journal of Computer Science and Network Security*, *12*(8), 74-83.

Ringold, A. R. (2014, June). *Command-and-control servers: The puppet masters that govern malware.* Website visited on 10-10-2016, via: http://searchsecurity.techtarget.com/feature/Command-and-control-servers-The-puppet-masters-that-govern-malware

Rowe, B. R., & Gallaher, M. P. (2006, March). Private sector cyber security investment strategies: An empirical analysis. In *The fifth workshop on the economics of information security (WEIS06)*.

Romanosky, S. (2016). *Examining the costs and causes of cyber incidents*. Journal of Cybersecurity, tyw001. http://doi.org/10.1093/cybsec/tyw001

State.gov. (2016). *Bureau of Economic and Business Affairs.* Website visited on 6-10-2016, via: http://www.state.gov/e/eb/index.htm

Urrico, R. (2015, September 11*). Government Launches Anti-Phishing Campaign*. Credit Union Times. Retrieved from http://www.cutimes.com/2015/09/11/government-launches-anti-phishing-campaign?slreturn=1476081013

The White House. (2014). *FACT SHEET: Safeguarding Consumers' Financial Security*. Retrieved from https://www.whitehouse.gov/the-press-office/2014/10/17/fact-sheet-safeguarding-consumers-financial-security

The White House. (2015). *FACT SHEET: Cybersecurity National Action Plan*. Retrieved from https://www.whitehouse.gov/the-press-office/2016/02/09/fact-sheet-cybersecurity-national-action-plan