Economics of Security — Security investment and Management

Tycho Teesselink (s1560506)
Tariq Bontekoe (s1451278)
Æde Symen Hoekstra (s1479679)
Ramon Houtsma (s1245228)
Group 13 — Phishing

October 2018

1 Methodology

1. Determine the problem owner by choosing one actor from assignment 1.
2. Choose a discriminating metric.
3. Plot the differences between problem owners w.r.t. this metric
4. Identify risk strategies to deal with the problem, also mostly w.r.t. the metric.
5. Think about other influencing actors
6. Think about what above mentioned other actors do/can do to tackle the phishing problem.
7. Look up facts and statistics that are needed for ROSI calculations.
8. Determine a loss distribution.
9. Calculate a ROSI using the found statistics, the dataset and the loss distribution.
10. Conclude.
11. Do a spelling check.

The rest of this draft contains the preliminary results of applying the methodology discussed above.

2 Problem owner

According to the Lean Six Sigma, the problem owner is the person functionally responsible for the process a team is trying to solve. In our case this would be the security consumers, i.e. the security decision makers. They interpret the results of the metrics and decide what action needs to be taken. More specifically they are the organizations and TLDs being targeted by phishing attacks. Organizations that are most likely to be frequently targeted handle personal data or online finances, because personal information can be sold and fraudulent transactions can be made when a user is compromised. This makes them an attractive target for attackers because of the quick return on investment for the attacker. TLDs also act as security providers because they deliver IT services and have the power to take down phishing sites.

In order to have a clear and unambiguous scope for this research we will only consider the organizations that are targeted by phishing as problem owners. The TLDs will be discussed, but as "other actors", with an influence on the security issue.

3 Relevant differences in performance

The time it takes until a known phishing site is taken down differs per targeted company. For some companies the average uptime is only a couple of days, whereas for others it is months. The variety in response time is enormous and could for most companies be

rigorously improved. The evaluation of this metric can be seen in Figure 1. Note that this graph only contains the companies with the highest average uptime, as otherwise the graph would be too large. We can see for example Mastercard, Visa, AliBaba and Post Denmark, have an average uptime of over half a year. However also lots of companies, not visible in this Figure, have an average uptime of less than 2 weeks, this includes companies like Paypal, Danske Bank, Wells Fargo and Halifax.

Often, the large response time affects the performance of security as the amount of time a phishing site is up, can greatly influence the amount of victims, although taking down websites is not a way to completely mitigate the security problem [1]. The problem owners should hence be open for a combination of approaches.

This variety of approaches can consist of detection methods for phishing sites or hiring a professional security company to detect and remove the infected domains. Another option is to take down the host instead of the domain name. The time to achieve this may vary widely because of different rules and regulations in different countries.

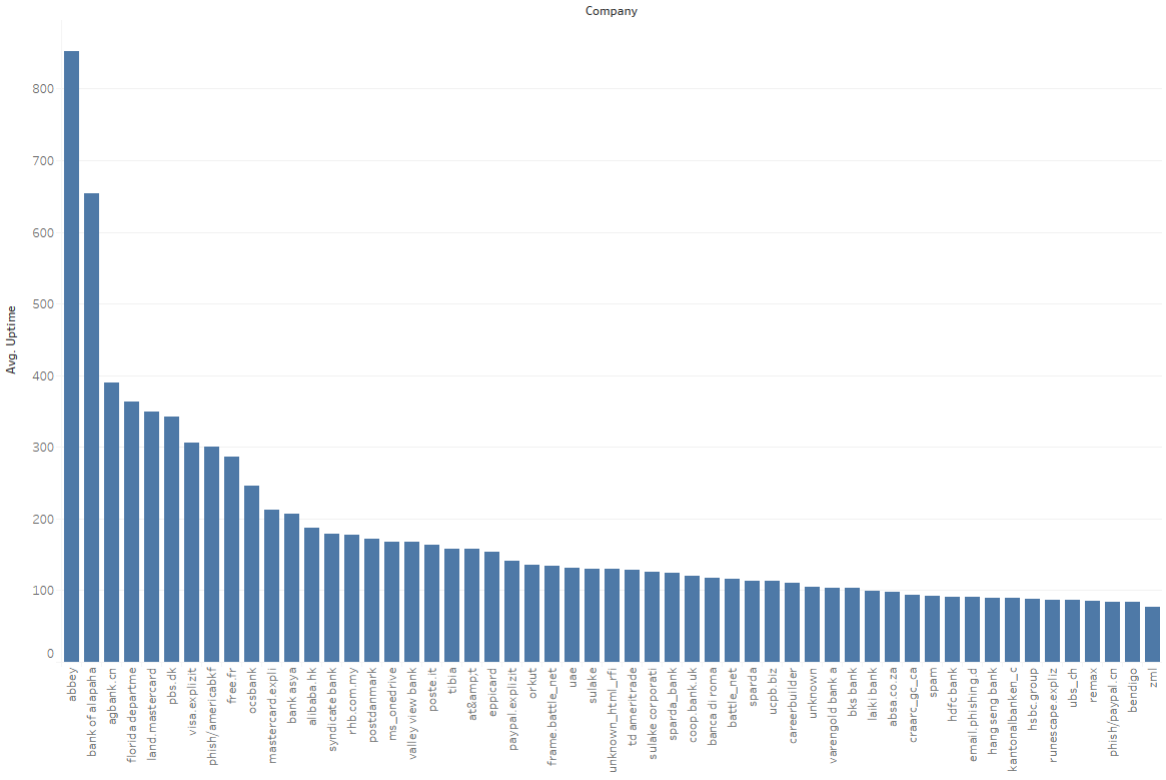

Figure 1: Average uptime (in days) of phishing sites per company.

4 Risk strategies for problem owner

The organizations with online services are the security consumers. The security issue of phishing has direct business impact because it is their clients that are targeted. The clients will be dissatisfied and may need to be compensated. We discuss four instruments in risk management to approach this security issue.

4.1 Risk mitigation

An incident response protocol that is executed upon materialization of a threat, in this case phishing. In this protocol actions that need to be executed will help in taking down a website as fast as possible. By taking down the phishing websites earlier, the risk of users being phished is less. Besides taking down the phishing websites, notices can be sent to all users of for example Paypal, that phishing websites are being used, and to pay extra caution when using their service.

Register domains that are similar to the domain name of the organization, purely to prevent phishing attacks from these domains. If these domains are unavailable for the attackers, less people will be phished and therefore the risk will be lower.

Use a smart intelligent phishing detection system, to scan new websites and have an early detection method to find phishing websites before they get used. In combination with the above mentioned incident response protocol, this might greatly lower the risks. An example of such a system for e-banking is mentioned in a paper by Aburrous et al. [2]

It is also possible to hire a company to detect phishing websites and to take them offline as quickly as possible. [3, 4] This way companies do not have to bother with hiring professionals themselves in order to develop detection models. Moreover, companies do not have to find out how they can take website offline. However, in this case it might still be useful for companies to have an incident response protocol, such that their customers can be warned when phishing risk for the clients of the company are high.

4.2 Risk acceptance

When accepting the risks, the party accepts that incidents will happen. The losses and consequences will be reimbursed by the same party. This strategy usually only attractive when the likelihood of threats materializing are low, or when the costs of reimbursement are lower than the costs of other countermeasures. A provider of e-banking will for example reimburse the losses due to fraudulent transactions of the consumer, if the account details have been stolen by means of a phishing website.

4.3 Risk avoidance

Strategies to avoid the risks of phishing include withdrawing from or limiting online interactions. This is not a viable strategy for organizations with core online activities. For example Paypal cannot simply stop facilitating online payment transactions as this is their sole business model.

4.4 Risk transfer

Transferring risk means that another party is responsible for the consequences of a materialized incident. An example of such a strategy is getting insurance. Since the data is based on phishing, the insurance party would reimburse any losses resulting from phishing and therefore the risk for the problem owners is transferred. This type of insurance does exist in practise, for example HDI has a program called Cyber+ Insurance [5], which covers losses caused by cyber crime and data breaches. This takes away most of the liability for the initial party, however, this will most likely come with a hefty premium.

5 Other actors

Five actors have been defined that can influence the security issue:

- Hosting providers
- Registrars / TLDs
- Website take-down services
- Online service consumers
- Insurance companies

6 Risk strategies for other actors

6.1 Strategies

6.1.1 Risk acceptance

Remaining risk that has not been mitigated by countermeasures will be accepted by hosting providers and registrars due to the fact that investing more money would yield negative returns. This is however conditioned on the fact that certain laws, for example about privacy, are being complied to by said mitigating measures.

6.1.2 Risk avoidance

Online service consumers may avoid the security risk by not using the online service. For example, they could go to the local bank to make payments instead of using online banking.

6.2 Have the strategies changed significantly over time in a way that reduces or increases risks?

In the early days, when phishing was being used for the first time, not many people were a victim. This means that the losses caused by phishing were also low. Installing counter-

measures were very expensive, and therefore it would be cheaper to accept the risk, and reimburse any losses due to phishing. However, when criminals started doing large scale phishing campaigns, the losses increased immensely and therefore the risk increased as well. This means that accepting the risks was no longer viable, and the strategy changed to mitigating the risk.

Another influencing fact here, is that technology became cheaper over the years. For example we have many machine learning methods that can help by identifying phishing websites, which makes it easier to decrease the uptime of a phishing website. Because mitigating risks is usually only viable as long as the costs do not exceed 37% (Gordon and Loeb), by decreasing the costs, we can increase the amount of risk mitigated. Therefore, over time, the fact that the price of technology decreases lowers the risk. If the price of a mitigating measure exceeded the costs of accepting it was better to accept than mitigate. This could now be changed to mitigating risk.

7 ROSI calculation for risk transfer strategy

Annual Loss Expectancy without security measures in place (ALE_0):
Annual Loss Expectancy with security measures in place (ALE_s):
Costs of security measure (c):

$$ROSI = \frac{ALE_0 - ALE_1 - c}{c}$$

The annualized loss expectancy (ALE) is the product of the annual rate of occurrence (ARO) and the single loss expectancy (SLE). It is mathematically expressed as:

ALE = ARO x SLE

The SLE is the cost per incident.

The annual loss expectancy of phishing in a mid-sized company is between $1,300,000 [6] and $1,600,000 [7].

A website-takedown service costs approximately $2000 plus an additional $1000 dollars per takedown. [8]

A piece of stolen personal or confidential data costs $158 on average. [9]

********** Work in progress ********

8 Conclusion

We conclude that something influences something else because of something

References

[1] T. Moore and R. Clayton, "Examining the impact of website take-down on phishing," in *Proceedings of the anti-phishing working groups 2nd annual eCrime researchers summit on - eCrime '07*. Pittsburgh, Pennsylvania: ACM Press, 2007, pp. 1–13. [Online]. Available: http://portal.acm.org/citation.cfm?doid=1299015.1299016

[2] M. Aburrous, M. A. Hossain, K. Dahal, and F. Thabtah, "Intelligent phishing detection system for e-banking using fuzzy data mining," *Expert Systems with Applications*, vol. 37, no. 12, pp. 7913–7921, Dec. 2010. [Online]. Available: http://www.sciencedirect.com/science/article/pii/S0957417410003441

[3] "Fraudwatch international – anti-Phishing Protection Services & Solutions." [Online]. Available: https://fraudwatchinternational.com/services/anti-phishing/

[4] "Sitetakedown – phishing Protection." [Online]. Available: https://sitetakedown.com/services/phishing-protection/

[5] HDI, "Cyber+ insurance: covers losses caused by cybercrime and data breaches," visisted on 26-09-2018. [Online]. Available: https://www.hdi.global/nl/en/insurance/cyber

[6] "Cost of cyber crime study." [Online]. Available: https://www.google.com/url?sa=t&rct=j&q=&esrc=s&source=web&cd=11&ved=2ahUKEwiFieiv8eTdAhUSPFAKHQCmBH0QFjAKegQIAxAC&url=https%3A%2F%2Fwww.accenture.com%2Ft20170926T072837Z__w__%2Fus-en%2F_acnmedia%2FPDF-61%2FAccenture-2017-CostCyberCrimeStudy.pdf&usg=AOvVaw0YtmuGNzmyIVFbQK8V1J1A

[7] "Survey reveals spear phishing as a top security concern to enterprises." [Online]. Available: https://blog.cloudmark.com/2016/01/13/survey-spear-phishing-a-top-security-concern-to-enterprises/

[8] "Sitetakedown – phishing Protection costs." [Online]. Available: https://sitetakedown.com/products/

[9] "IBM 2016 Cost of Data Breach Study - United States," Apr. 2017. [Online]. Available: http://www.ibm.com/security/data-breach/