Assignment block 3 - Draft

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

A problem owner is affected by the security issue or benefits from the solution to this issue [?]. The security issue discussed is phishing. There are several problem owners that can be defined regarding this security issue:

-          Firms

-          Customers

-          E-mail providers

-          Law enforcers

Firms are obvious owners of the security issue. Since they are being targeted by the attackers, they are the biggest problem owners. They are also the ones who have to take the most security measures against these attacks.

The customers are the second type of problem owners mentioned. Phishing websites attack firms through their customers, because the customers are then ones who end up using the phishing websites. Therefore security measures can also be made from the customers’ side.

The third type of problem owners mentioned is the e-mail provider. This because most phishing websites are accessed through an email. E-mail providers carry the issue in this way, but since this isn’t mainly their concern, they do not take a lot of measures against these e-mails. At most a filter is added, which tries to distinguish the phishing e-mails from the regular ones. Therefore e-mail providers are not part of the main problem owners.

The last type of problem owners mentioned are the law enforcers. Phishing is a crime, therefore law enforcers are also a part of this security issue. Although phishing is a crime, it is not (in most cases) a severe crime. Law enforcers rather spend their time and effort at more severe problems [?]. Therefore law enforcers are also not considered a part of the main problem owners.

In the first assignment, the focus was laid on the perspective of the targets of the phishing websites. Useful metrics and measurements were made and one could derive for example the security level of a target based on the average up-time of the phishing websites corresponding to the target.

Using this information the obvious problem owner of the security issue as measured in our first assignment would be the targets of the phishing websites. Looking at the data and specifically at the targets of the phishing websites, it can be seen that most of the targets are either banks or other financial transaction organisations. This is an obvious finding, since the main goal of the attacker is to acquire money [?].

Because of this finding and because it makes this assignment a lot more relevant, the focus in this assignment will be laid on the *banks and financial transaction organisations affected by the phishing websites.*

In The Netherlands, most banks offer financial compensation for victims of phishing, unless they have been very neglectful, even if they are not always obligated to do so. It is the responsibility of banks to warn their clients against phishing tactics [1].

The loss for the targeted organizations does not only consist of the direct costs of compensating victims of phishing, but a high number of incidents may affect the reputation of the organization and it may decrease the willingness of its customers to use internet banking or other digital services. Consumers see security as a commodity. The CSO of PayPal, one of the world’s most often targeted organizations, said that phishing is an overestimated threat and that it’s not even in the top 5 threats [2].

We could think of the concept of network externalities in relation to phishing, but it seems like a phishing incident is as bad for the targeted organization as for the actual consumer/victim. The phishers however, use money mules to shift the costs of being caught unto them, by letting the mules transfer the money to them via non-refundable operations. In this way, the mule is liable for the costs.

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

The most interesting differences are probably the high amount of phishing websites in Chile and low amount in China. According to a report of the Anti-Phishing Working Group, around 85% of the malicious domain registrations were registered to phish Chinese targets [3]. I have no idea how to explain this, maybe they have other data, but from where?

(Not done yet)

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

In the lecture is explained that business drives security strategies for security providers. Security is not the core competence of security providers.

The lecturer mentions that the economics of information goods create an environment with significant network externalities and economies of scale. Because the expenses for developing software are sunk costs, it is rational to ship the product as early as possible and to add security features later.

However, although this might be the case for very new companies or services, for banks this is a little different. Banks have been providing services in which security is a core feature for many years, in fact people put their money on a bank to keep it safe and to get financial services. People do not want to try internet banking unless they are convinced of the security of it. On the other hand, eBay is a company that is targeted very often by phishers and this fits the lecturer’s description a lot better.

There are 4 strategies the problem owner can follow to reduce the security issue.

Firstly the banks and financial transaction organisations can apply risk mitigation. This is an important strategy. Risk mitigation tries to reduce the likelihood and severity of loss events by protecting vulnerable assets with technical and organisational measures [?]. This can be done by for example, find and remove the phishing websites, educate the customers in order to prevent them to use the phishing websites or find and stop attackers creating the phishing websites. This strategy is practiced, but because of the numbers involved (costs, attacks) it is not very profitable for an organisation to put a lot of effort in this strategy [?].

The second strategy discussed is risk acceptance. Overall this is done quite a lot [?]. For big companies such as PayPal, a lot of phishing websites are created throughout a small period of time. It is hard to mitigate at a high level. The obvious measure a bank can take is to better educate their customers about phishing. But there will always be old/not-very-smart people that fall for the deceit. So to some extent it is not profitable to put much effort in mitigating this issue [?].  Therefore most strategies consists of accepting this issue. This is often combined with some sort of compensation for the customer involved in the attack.

The third strategy is risk avoidance. This is very hard in this case. In order to avoid the risk, one would have to remove the features which are being exploited, such as online banking or online payment systems. Since these are big features which are very convenient for the customers, and are excessively used, it is unthinkable to remove these features.

The last strategy is risk transfer. The impact the organisations experience are mostly indirect impacts. Attackers don’t focus on the organisation but on the customers. Because the customers play an important role, risk transfer also has its role in the overall strategy. This is done by policy specifications [?]. Because the attacks are customer driven, the organisation can’t always be held responsible for the incident. Therefore every organisation has its policy specification regarding phishing attacks, which can decide who is responsible for the incident. Since organisations can exploit this …, there are also certain laws towards this issue. For example in The Netherlands, if a bank did not warn a customer enough about phishing, they are required to compensate the customer in case he/she becomes a victim [?].

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

There are a big number of actors involved in the phishing issue. The most important are:

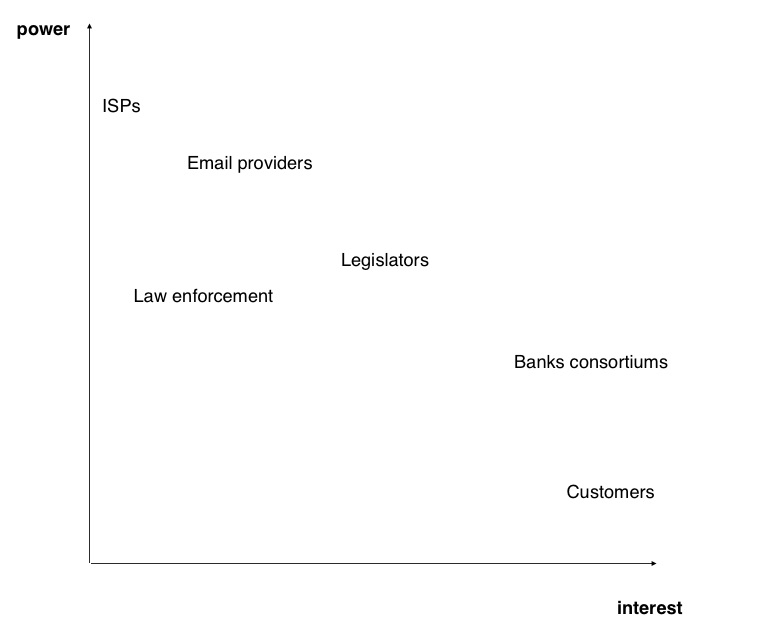
Bank customers: they might be involved in two ways. If they don’t have any risk transfer measure in place they will actually lose their money. Even if they do not lose money personal costs associated with attacks include loss of time, stress, decreased trust and use of the internet (Dhamija & Tygar, 2005; Hardee, West, & Mayhorn, 2006) and embarrassment.

Law enforcement: they are obviously involved since they are supposed to stop the problem and arrest criminals.

Consortiums of banks: banks usually cooperate in order to tackle common security problems.

Internet Service Providers: they are marginally damaged since a share of their resources, even if very small, is used by someone else to gain illicit profit.

Email providers: similarly to ISPs a percentage of their resources is used by criminals. For example they spend resources to store in servers all their clients emails, including phishing emails.

Legislators: they are supposed to decide how to solve the problem of phishing from the legal perspective (how to punish criminals, cooperation agreements with other countries etc)

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

**·         are there actors with different strategies? why?**

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

Bank customers: customers can just decide not to use internet banking (risk avoidance). Often customers have some form of risk transfer in place, usually in the form of a legal agreement with the bank when they sign the contract to get a bank account.

Law enforcement: risk acceptance. Since they have limited resources they have to accept that a component of the risk could realise.

Consortium of banks: risk reduction. For example by awareness campaigns, meetings where best practices are discussed, cooperation agreements (information sharing especially) etc.

ISPs: they do not have incentives to use risk reduction, since they do not suffer the consequences of phishing. They could do a lot though like analysing traffic and locating sources of phishing.

Email providers: risk reduction. For example with the use of anti spam filters. Similarly to ISPs they are hit only marginally by phishing, so they do not have enough incentives to do more.

Legislators: risk reduction. For example by awareness campaigns, development of specific policies and laws. As for law enforcement there is a form of risk acceptance (government can’t invest every resource it has in order to 100% eradicate phishing).

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

**·         Estimate the costs involved in following that strategy**

**·         Estimate the benefits of following that strategy (assume a particular loss distribution)**

The cost of security consists of two parts: direct costs and indirect costs. Expenses for acquisition, deployment and maintenance fall under directs costs, while productivity loss falls under indirect costs.

It is more difficult to determine the benefits of a security investment, as their goal is to prevent losses. Whether and how much an organization loses, depends on the behavior of the attacker. Usually, the marginal benefits of security investment decrease.

One of the strategies that the problem owner can follow is risk acceptance. Banks often reimburse their clients who have fallen victim of phishing, but they cannot always prevent it. The global losses from phishing were around $1.5 billion in 2012 [4].

There are no costs for risk acceptance, but there are also no benefits. In this case, risk acceptance is applied because, as customers are the primary target for an attack, there is not much a bank can do about the problem.

**Sources:**

This is a very interesting paper that states that phishing is not as profitable as it seems and that the losses of phishing are overestimated. *A Profitless endeavor: phishing as tragedy of the commons :*<http://dl.acm.org/citation.cfm?id=1595686>

This is very useful information: http://www.ingentaconnect.com/content/aea/jep/2009/00000023/00000003/art00001

[1] About compensation for victims of phishing (Dutch):<http://www.geldenrecht.nl/artikel/2013-08-19/geen-compensatie-voor-phishing-slachtoffer>

[2] PayPal CSO: Phishing threat overstated: http://www.darkreading.com/attacks-breaches/paypal-cso-phishing-threat-overstated/d/d-id/1128582

[3] APWG: http://docs.apwg.org/reports/APWG\_Global\_Phishing\_Report\_1H\_2014.pdf

[4] http://www.emc.com/collateral/fraud-report/online-rsa-fraud-report-012013.pdf