Review for group 11, from group 8

Summary

The paper examines security strategies to cope with the hacking of websites. A hacked website can not only be bad for the website owner, but also for the hosting providers' business. There are countries that are more vulnerable to hacker attacks than others. This enabled group 11 to create possible strategies to ensure better protected domains in cyberspace. The strategies that have been defined can not only be incorporated by the hosting provider, but for other actors as well. The actors that are defined in the actors section are: Consumers, Website security industry, and Governments. For these actors, strategies are defined in order to reduce the security risks and costs. The drawbacks for all these strategies are the costs of implementing them. For a case study on TinyURL, the ROSI is 25.57%. The risk mitigated in this case is 85%.

Nice parts

- The table at the end of section 3 gives a really nice overview of what was discussed in the chapter.
- It is nice that you found data instead of having to assume a lot. All data has been backed up.
- Good, extensive overview on the losses due to the risk exposure and the costs of implementing the mitigation strategies.
- Nice conclusion, identifying the shortcomings of your ROSI calculation as well as giving further recommendations.

Major issues

None

Minor issues

- The strategies use actors that are not explicitly defined in the actors section. It is stated that for example Hosting Providers can be defined as security consumers, however, these terms are not stated in the actors section.
- The usage of 85% as a percentage mitigated seems rather vague. It can very well be that this is a common percentage used in literature, but it would seem more applicable to fit this percentage to your devised strategy instead of directly assuming this from theory.
- Consumers and customers is used interchangeably, but hosting provider is also called a security consumer. This makes certain parts of the report hard to read.
- The TinyURL case uses mitigation strategies, but the link between strategies defined by the group and these strategies is not clearly defined.
- It is assumed that code review is free. However, this costs a non-negligible amount of time which in turn results in a loss of productivity which can be very high in fact.
- The cost for implementing controls like SSL, DDoS protection and antivirus software, including maintenance for only 426.38 euros per year is quite low. It probably takes more than a week to install all of this, so the person installing the controls would already cost more than the total amount.