Summary

The document designs metrics for sales on underground forums and criminal organizations online. The stakeholder is a national government-based security organization. It is vital to have good metrics in a government-based organization because resources to start an investigation are scarce. The value that is threatened is information such as stolen credit cards, email accounts etc and the health & well-being of Dutch Citizens, due to the proliferation of illegal drugs and weapons. The party that is affected are the normal internet users and also Dutch Citizens.

Ideal metrics for these internet organizations include incident details, mitigation actions and assets involved in the incident. To implement metrics in practice, textual analysis is needed. During the textual analysis, the data is parsed for key features. It can prove difficult to implement such metrics, mainly due to the fact that textual analysis is not yet exhaustive. Security groups and academic groups have both defined metrics to be used in practice. There was a study where different post were defined in order to parse and analyse the text. The authors of the study partnered with twitter to further track the fraudulent accounts.

The metrics defined by the group are:

1. Sales by volume of product
    a. This metric examines relative percentages of revenue. This does not reflect the amount of products sold as some products might be more expensive than others.
2. Sales revenue over time
    a. This allows to see a trend in the total sales revenue.
3. Product sales trends
    a. This allows to see a trend in sales of specific products.

The dataset has limitations, the main limitation being that textual analysis is needed in order to analyse the data.

Evaluation

The group defines a clear thesis, but there is not a real solid argument. The security issue is well defined. The dataset is analysed according to the stated thesis, however, the way that the dataset is analysed does not give measurable metrics to measure security. The metrics mainly give insight to what is happening, rather than making it easy to compare different jurisdictions (as it is a government-based agency).

Strengths of the assignment

- Stakeholder is clearly defined.
- Metrics used in practice are well explained. There has been thorough investigation on this topic.
- For all the metrics, the group provides ways to improve on them when more data becomes available.

- The report is nicely written in report style; every chapter has a small introduction, which is good.
- The shortcomings of their metrics and the dataset are discussed before the conclusion.

List of major issues

No major issues were identified.

List of minor issues

- There are very little ideal metrics defined.
- The amount of metrics defined is rather low, there is a mention that this is only a small part of what can be developed using this data. The metrics mentioned could have been evaluated.
- The report does not substantiate why the defined metrics are appropriate to measure the security of a government-based organization.
- The metrics on revenue trends per country could be normalized with the number of internet users from it, so that a realistic comparison could be made between the trends of different countries.