Draft Assignment 1 Block 2 - Group 11

1. What security issue does the data speak to?

Nowadays, almost 3,7 billion people around the world use mail accounts (Tschabitscher, 2017). All these accounts are sensitive to attacks from criminals, for example through sending malicious links that allows viruses to install on your computer, or targeting bank accounts by tricking out personal information via false websites and links. Spam earnings by the operating criminals may ran into the millions per year in 20102. Furthermore, the victim experiences direct and indirect losses in form of money, loss of productivity and innovation (Ganan, 2017). Part of these losses are spent on spam filters. These filters are the first defence for protecting mail accounts from these aforementioned threats (Ganan, 2017).

To help decision makers in the field of security in businesses and institutions, data about spam incidents can be studied to better secure the users of internet from criminals. The findings should then be put into an economical context to be able to understand the real benefits and costs that both private parties and society as a whole have to deal with. Some metrics that form this economical context have only been established in the last few decades. We will take a critical look at the metrics composing the security level which would be useful for decision makers, specifically when it comes to securing against spam which delivers malware. This is done by using a dataset which contains the events of prevented delivery of spam containing links to malware. The dataset comes from CleanMX, which is a small company which offers an email spamfilter service to individuals and organisations. The dataset from CleanMX which we have obtained, lists the incidents of filtered out spam as: date, time stamp of detection, and the URL in the email which located malware according to the spamfilter. The dataset spans all reported incidents over three years; from 1 January 2014 to 31 December 2016. We will use this dataset to evaluate our metrics of security level which we form from literature. We will try to optimise these metrics on their expected use for decisions regarding the performance of malware spam filters as a control mechanism for optimising security benefit.

2. What would be the ideal metrics for security decision makers?

As described by Bohme, the ideal metric would enable decision makers to compare alternatives associated with a certain security level, for which he generated the following formula (Bohme, 2010):

ROSI (Return on Security Investment) = (benefit of security - cost of security) / cost of security.

Cost of security is defined by several decompositions in literature. Anderson et al. decompose the cost of cybercrime into three categories: direct losses, indirect losses and defence costs (Anderson et al., 2012). Direct cost are “the monetary equivalent of losses, damage, or other suffering felt by the victim as a consequence of cybercrime” (Anderson et al., 2012, p.5). Indirect losses are “the monetary equivalent of the losses and opportunity costs imposed on society by the fact that certain cybercrime is carried out” (Anderson et al., 2012, p.5). Defence costs are “the monetary equivalent of prevention efforts, which includes the direct defence costs (development, deployment, and maintenance) as well as the indirect defence costs (inconvenience and opportunity costs caused by the prevention measures” (Anderson et al., 2012, p.6). The virus scanner CleanMX belongs to the category defence costs. An example of the indirect defence costs of the CleanMX are the costs associated with training the staff and installing the service. The direct defence costs of the CleanMX can be defined as the following explanation of Carlos Ganan, who argues it is attractive to capture impact of cybercrime in a monetary amount, making it comparable and amenable for decision making, but it is actually impossible to generate trustworthy monetary estimates (Gañán, Ciere, & Eeten, 2017). Ganan et al. argue cybercrime has different impacts to individual agents (Gañán et al., 2017). CleanMX is a spamfilter, this means the client would anticipates on attackers. When using CleanMX, a client would have direct costs on (1) buying the product and (2) assessing the security by a managing board. Also, indirect costs can be indicated when using a spamfilter, such as productivity losses due to inconvenience of using the software. For example, spam filters possibly need to be updated every once in awhile, which will cost time. Above mentioned impacts of using CleanMX are short-term and based on individual users. Ganan et al. also described different possible impacts for long term, which burdens an economy or sector (Gañán et al., 2017). At this stage of the study, this will not yet be described.

As explained by Carlos Ganan, benefits of security are determined by the prevented accidents (in our case, prevented by the CleanMX system) and dependent on the value of the assets at risk (Ganan, 2017). However, fewer accidents can either be due to more attacks failing (better security) or due to fewer attacks (change in attacker behavior) (Ganan, 2017). To determine whether a decrease in attacks is due to change in attacker behavior or due to better security, we are therefore required to control for the attacker behaviour and for the differences unrelated to security (Van Eeten, 2017). Ideally, the CleanMX data should be compared with other spam filters/virus scanners to determine of the amount of the attacks is overall decreasing or specifically decreasing for this specific security system. Moreover, Noroozian et al. mention that there should be controlled for 'the level of exposure', which they define as "the degree to which a provider, or another class of defenders being studied is exposed to a certain threat" (Noroozian, Ciere, Korczy, & Eeten, 2017, p.4). Controlling for the level of exposure includes controlling for the size of the provider, as "larger hosting providers have more customers and hence a higher probability of one of those customers being compromised" (Noroozian et al., 2017, p.4), and controlling for the business model of the hosting service, as "customers of cheap hosting services running popular content management systems are more likely to be compromised than professional hosting customers with their own security staff" (Noroozian et al., 2017, p.4).

Figure 1 shows the relationship between the level of security, the number of incidents, the number of prevented losses and the benefits of security. A negative relationship means that an increase of the one factor leads to a decrease of the other factor, and vice versa. For example, an increase of the level of security should lead to a decrease of the number of incidents. A positive relationship means that an increase of the one factor leads also to an increase of the other factor, and vice versa. For example, an increase of the level of security is associated with an increase in the number of prevented losses. The dotted arrow between prevented losses and incidents indicate that the number of prevented losses are dependent on the number of incidents. As it is not possible to directly measure the level of security, the decision maker would like to measure indicators that reflect different aspects of the security level. Ideally, in case of the CleanMX spam filter, the type of security metric to measure the security level would be a metric based on incidents and prevented losses in order to evaluate the performance of such control mechanism. As the data provided to us attains the data and web links associated with incidents occurred over two years period, the performance of the CleanMX spam filter can be indicated by the decrease in incidents/prevented accidents. Ideally, the decision maker would like to know the factors influencing the incident rate, so he could try to control them (for example, by improving the spam filter). However, as explained by Noroozian, using abuse data to measure security performance suffers from the problem that abuse data is "driven by a multitude of causal factors that are hard to disentangle" (Noroozian et al., 2017, p.1). Besides, abuse data is "notoriously noisy; highly heterogeneously; often incomplete, as not all abuse events are observed; and biased, as providers without incidents were not observed" (Noroozian et al., 2017, p.2).

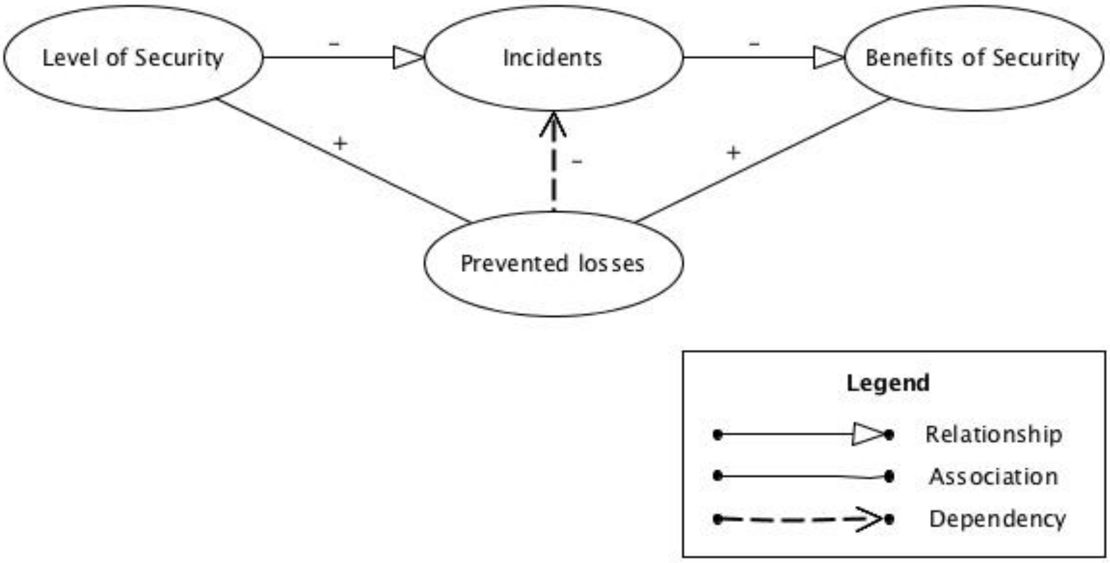


Figure 1: Relationship between the level of security, incidents and the benefits of security

3. What are the metrics that exist in practice?

Nooroozian et al. noted four problems with incident data, and abuse data in specific: the data are noisy, comparison of data is difficult due to heterogeneousness, possible biases in datasets, and the multicausality of the incident data (Noroozian et al., 2017). Taking into account these problems with incident data, Nooroozian et al. created a statistical model which could quite significantly predict a variable that they called "security performance" among different hosting providers (Noroozian et al., 2017). Simplified, the model they use, takes an aggregate of different factors of exposure of the subjects (the hosting providers), a random error variable for number of attacks, and an input variable of incident count, to output the security performance (Noroozian et al., 2017). Testing their model they are able to show that using this model the security performance explains most of the variance in the incident count (Noroozian et al., 2017).

Following Nooroozian, for each dataset the number of observed events per provider is counted. This metric is defined as the number of unique pairs (domain-IP-address) recorded per abuse feed and uses Autonomous Systems (AS) as unit of analysis (Noroozian et al., 2017). Even better is to, if possible, use the organization from to which the IP-addresses are assigned. Important is to note the observation bias in the data, especially with one dataset. The following events per dataset can for example be noted: Alloctated IPs, Domains, Hosting IPs, Shared IPs and Shared Domains. These events can be translated into a latent variable, that defines the level of exposure of the dataset. Nooroozian argues that if we can control for a random variable, then the main driving factor in the abuse data is the security performance (Noroozian et al., 2017).

4. A definition of the metrics you can design from the dataset

We are going to look for different patterns/trends in the data over time, to enable evaluation of the performance of the CleanMX. Table 1 provides an overviews of all metrics defined for the purpose of this case in an attempt to understand any changes of the attackers behaviour by examining different factors like different domains or the time of the attacks.

Metric	**Definition**
Incidents per time (year, per 6 month, per season)	Examine the #incidents in different time periods can be used to identify time periods where had an unusual behaviour (more/less incidents than usual #incidents)
Number of Incidents at Day (8:00 - 20:00) VS Number of Incidents at Night (20:01 - 7:59)	Give an insight on attacker behavior, do they send more attacks during day or during night.
Incidents/Internet Users	Examine if there is a dependency between the #incidents and the total number of Internet User. What it means for the number or incidents if they exist more users? Does it go up?
Number of Incidents per Domain	Frequency of Domain Appearance, how many incidents had the same domain as target. Example of Domains: .com , .mobi etc
Number of Unique Domains	How many Unique Domains exist and does their appearance be a random event based on the number of incidents
Number of Incidents per file type (.php, .gif etc)	Frequency of File Type Appearance how many incidents had the same file type. Example of Domains: .html , .php etc.
Number of Unique File Type	How many Unique File Type exist and does their appearance be a random event based on the number of incidents
Number of Incident per Service	Frequency of Service Appearance how many incidents used the same service. Example of Domains: facebook.* , diet.* etc.
Number of Incidents per Country	Examine how many incidents occurred per country using the domain of each country (.nl, .au, etc.)

Table 1: Overview of Metrics

5. An evaluation of the the metrics you have defined. This should include graphical representations of the metrics (e.g., histograms, scatter plots, time series, bar charts).

A. Historical trend: incidents changing over time?
B. Difference in type of links: html vs php etc. -> count attacks
C. Check the domain: are there interesting patterns to find?
D. Is there any pattern to find per day? Clustering on a daily basis -> Cluster using type(php/html etc) with time or year -> trying to find patterns (same time, same year etc) between file

with the same type possible results attackers had a specific target (file format) over a specific time period.

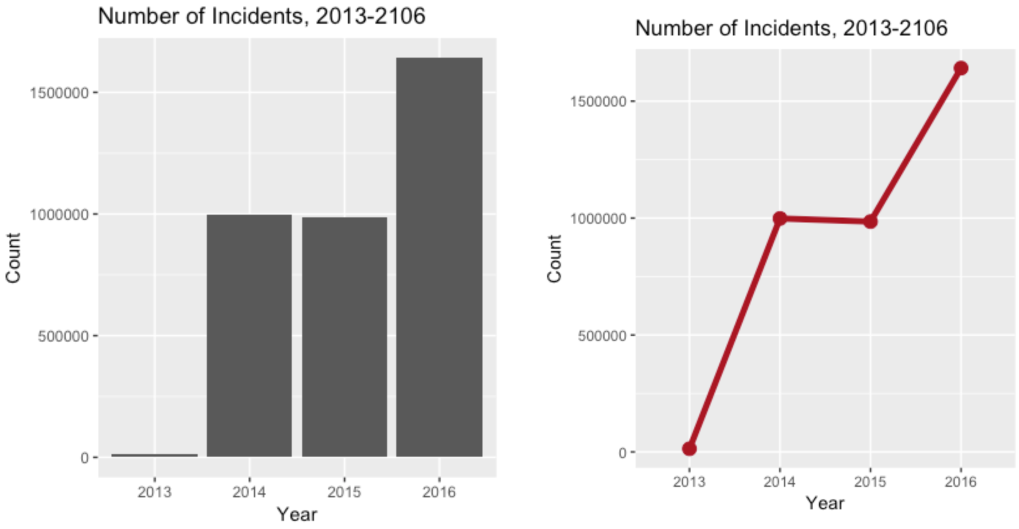


Figure 2: Total Number of Incidents per year

Looking at Figure 2 where the total number of Incidents is presented, values from 2013 appeared to have a massive difference in the number of Incidents compared to other values. This is occurred due to incomplete and missing values from datasets available. As a results values from 2013 are considered noise or outliers in the dataset and would be removed. Values from 2014 and 2015 show that the number of incidents is steady but the value from 2016 shows a big increase at the number of incidents and should be examined in more detailed when this increase happened. Looking at Figure 3 it appears that the increase of the incidents happened at the end of 2015 between months (August and December of 2015) but at the first half of 2016 it appears that the number of Incident went down and had similar value as previous values over time. Due to the incompleteness and missing information from the dataset, it is difficult to estimate if the increased happened because attackers changed their behavior, more user were targeted or CleanMx control wasn't working properly, same can be said also for the decrease.

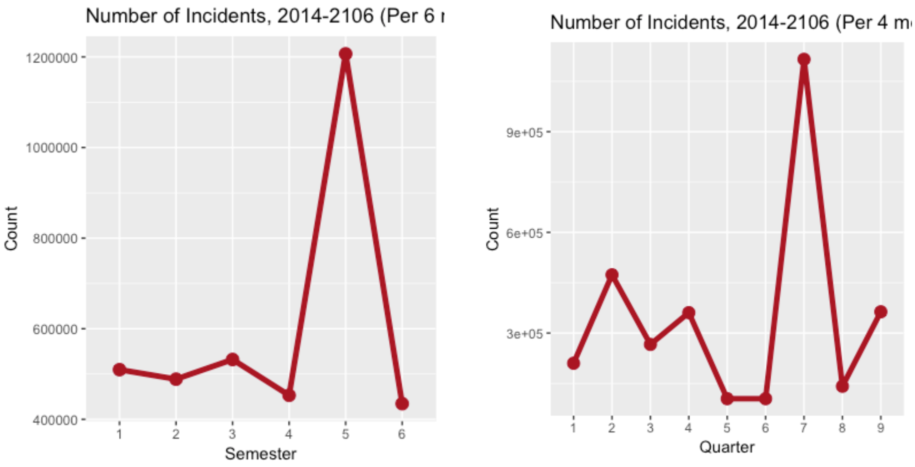


Figure 3: Number of Incidents per 6 months (right) and per 4 months (left)

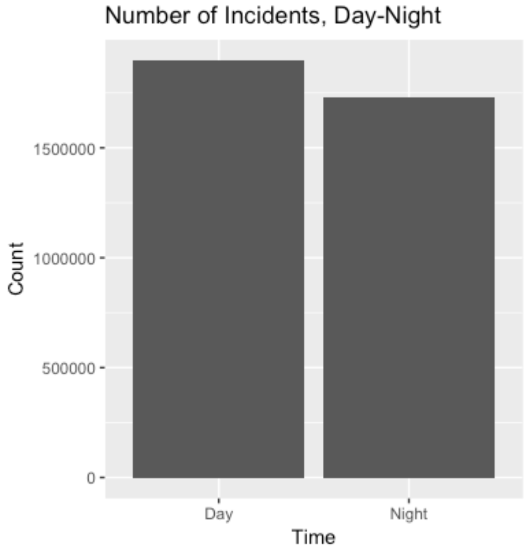
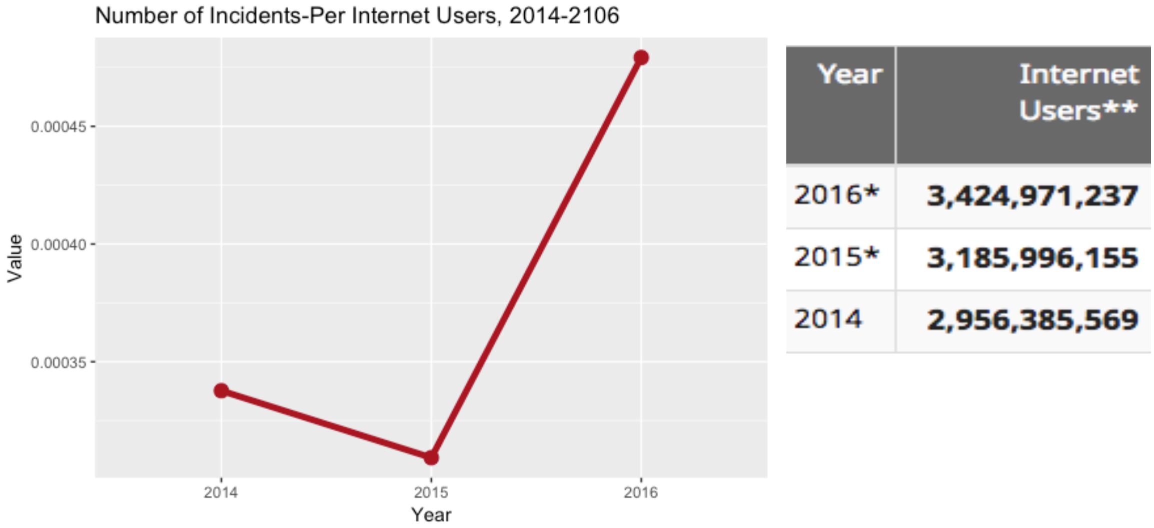


Figure 4: Number of Incidents Day VS Number of Incidents Night

Figure 4 presents the results regarding the time of incidents happened. Day values are about incident happen between 8:00 and 20:00 while night values are incidents between 20:01 and 7:59. Day hours have 168474 more incidents in total than night hours.



Year	Internet Users**
2016*	3,424,971,237
2015*	3,185,996,155
2014	2,956,385,569

Figure 5: Incidents Per Internet User

Obtaining data regarding the use of Internet (InternetLiveStats, 2017) in Figure 5 is presented the changes in the number of incidents per user over the time period. In 2016 there were more incidents per user than the two previous year. But by looking the Table showing internet user, it is concluded that the number of users in the case of CleanMx doesn't necessarily means and more incidents since in 2015 there were more internet users and fewer incidents comparing them to 2014. It can be concluded that the number of internet users in general cannot give insights about the incidents and the attacker behavior.

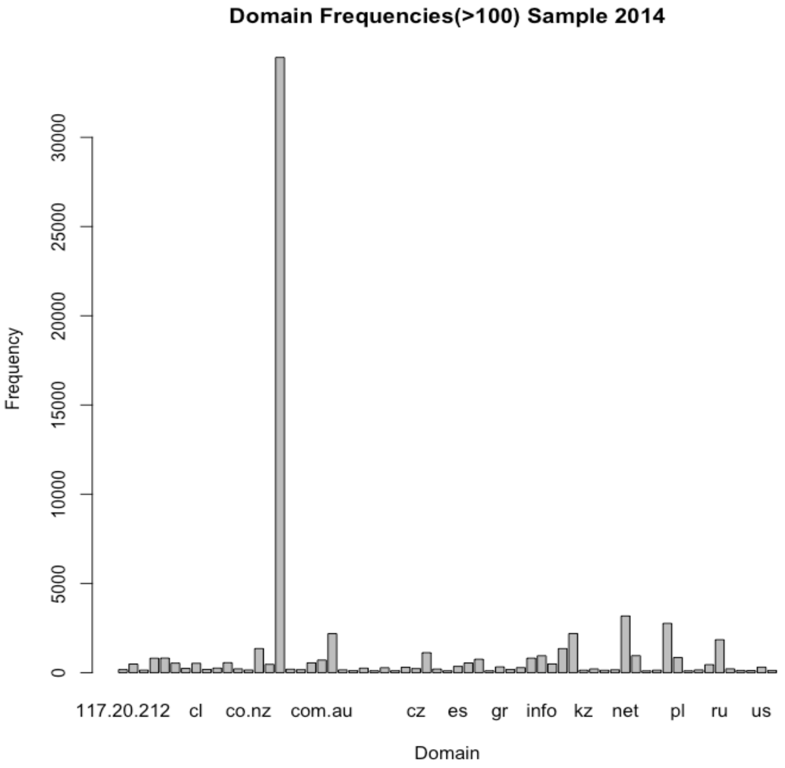


Figure 6: Frequency of Domain in a Sample Set of 214

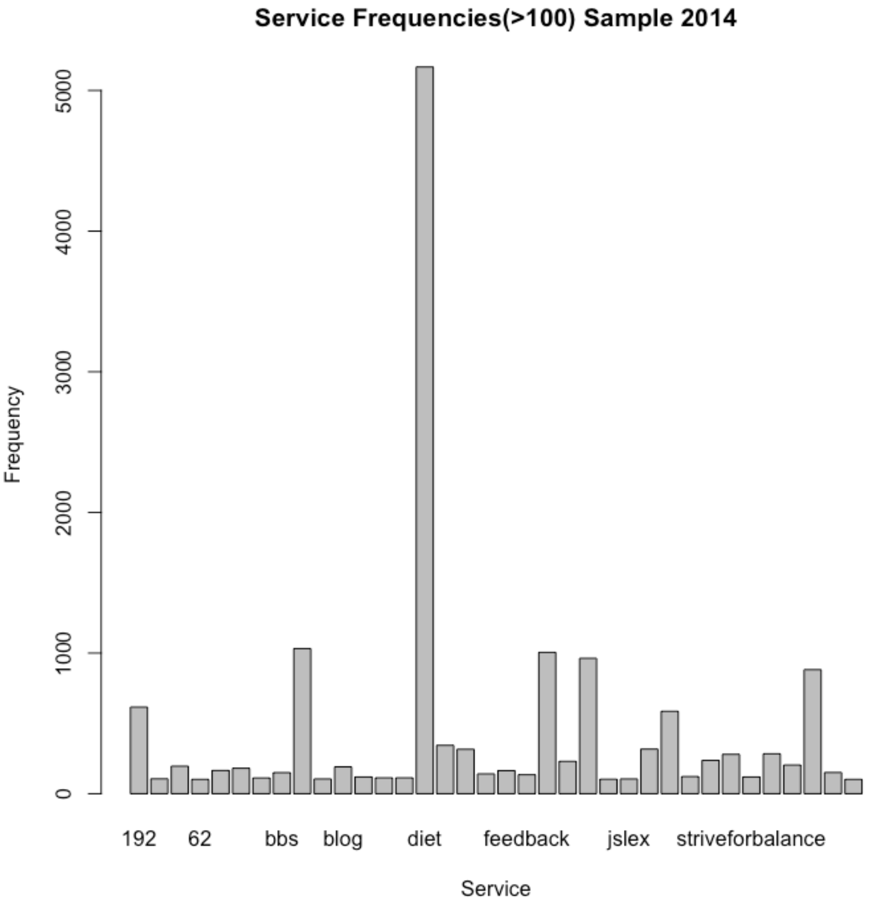


Figure 7: Frequency of Service in a Sample Set of 214

6. References

Anderson, R., Barton, C., Rainer, B., Clayton, R., Eeten, M. J. G. Van, Levi, M., … Savage, S. (2012). Measuring the Cost of Cybercrime. *WEIS*, 1–31.

Bohme, R. (2010). Security Metrics and Security Investment Models. *Advances in Information and Computer Security, Lecture Notes in Computer Science*, *6434*, 10–24.

Ganan, C. (2017). Tutorial block 2 measuring cybersecurity - WM0824 Economics of Cybersecurity TU Delft. Delft.

Gañán, C. H., Ciere, M., & Eeten, M. Van. (2017). Beyond the pre y penny : the Economic Impact of Cybercrime. *NSPW 2017*. https://doi.org/10.1145/nnnnnnn.nnnnnnn

InternetLiveStats. (2017). Internet Users. Opgeroepen op 09 17, 2017, van internet live stats: http://www.internetlivestats.com/internet-users/

Noroozian, A., Ciere, M., Korczy, M., & Eeten, M. Van. (2017). Inferring the Security Performance of Providers from Noisy and Heterogenous Abuse Datasets. *WEIS*, 1–26.

Tschabitscher, H. (2017). Can You Guess How Many People Use Email Worldwide? (It's Astonishing!). Opgeroepen op 09 18, 2017, van Lifewire: https://www.lifewire.com/how-many-email-users-are-there-1171213

Van Eeten, M. (2017). Tutorial block 2 measuring cybersecurity - WM0824 Economics of Cybersecurity TU Delft. Delft.