Dana Dülcke / Julia Kleinschmidt / Olaf Tietje / Juliane Wenke (Hrsg.):
Grenzen von Ordnung. Eigensinnige Akteur_innen zwischen (Un)Sicherheit und Freiheit
ISBN 978-3-89691-852-9

Gerd Beuster

Threat Modelling and Risk Mitigation – An IT Security Perspective

1. Introduction

The goal of IT Security is to protect both data itself and the processes for manipulating data. For example, a bank wants to protect the data of its customers (which are often a direct representation of monetary assets, for example the balance of an account), and the processes manipulating this data, like money transfers. The items to be protected are known as 'Assets'. 'Threat' is another main category in IT Security. Starting with a set of assets to be protected, professional IT Security engineering identifies the threats to the assets and how to counter these threats.

As a professional field, IT Security focuses on institutional actors like large companies and states. Protecting non-profit oriented entities is not a typical focus of IT Security research. As a result, protection mechanisms for individuals and small and informal groups are less developed. Here we typically find ad hoc advices like 'one should not post personal information on the Internet' or 'one should use encrypted email'.

Due to a lack of systematic security analysis, it is not clear if and when these security advices are applicable, and if they are sufficient. This paper shows how the methods of professional IT Security modelling and analysis can be tailored towards individuals and small groups of people. It shows how the systematic threat analysis approach of professional IT Security methodologies can be used to improve the IT Security of an environmentalist group as an example for a small and informal group with a threat landscape significantly different from the typical targets of IT Security threat analysis.

2. IT Security Basic Principles

The IT Security community agrees on the following *basic principles* (cf. Pfleeger/Pfleeger 2013: 10ff; Stallings/Brown 2012: 32ff; Ellis 2013: 1033ff):

- Confidentiality
  Confidentiality means that information must not be disclosed to unauthorized parties. ISO 27001[1] defines confidentiality as "the property that information is not made available or disclosed to unauthorized individuals, entities or processes" (ISO/IEC 27001 2011: 2).
- Integrity
  Integrity means that information must not be manipulated. ISO 27001 defines integrity as "the property of safeguarding the accuracy and completeness of assets" (ISO/IEC 27001 2011: 2).
- Availability
  Availability means that information must be accessible when it is requested by an authorized party. ISO 27001 defines availability as "the property of being accessible and usable upon demand by an authorized entity" (ISO/IEC 27001 2011: 2).

IT Security is about protecting information. For example, the information 'I am willing to pay 5,000 Euro for your car' should be protected in respect to integrity. It is important that nobody can manipulate the message and thus make me pay 50,000 Euro instead of 5,000 Euro. Typically, confidentiality of the information is not an issue in such a case. On the other hand, a physician's data about a patient must be protected in respect to confidentiality, integrity, and availability: Nobody except authorized personnel should know about the medical conditions of the person (confidentiality). It must not be possible to manipulate the patient information (integrity). They patient information should be available when needed (availability).

3. Security Guidelines for Individuals and Small Groups

This paper addresses threats to individuals and small groups and suitable counter-measures against these threats. As an example, it shows how IT related threats and counter-measures for a fictitious environmentalist group can be modelled. This is a suitable example, because such a group is subject to a large variety of threats: The kind of threats cover both confidentiality (for example, who is a member, what activities does the group plan?), integrity (for example, how can

1 The ISO/IEC 27000 family defines international standards for IT Security. From this family of standards, ISO/IEC 27001 defines requirements for Information Security Management Systems. National schemes like the German *IT Grundschutz* adapt ISO/IEC 27000.

the authenticity of published statements be ensured?), and availability (how can the group stay operational even when faced with oppression?). There is also a large range of threat agents, ranging from more or less skilled individuals (for example a group member's boss who does not approve of the activities of the group or an individual with opposing views) to large organizations like national states and large corporations.

When planning actions, the group members use laptops and email. The group will probably use more IT equipment (for example a website to spread information). However, this paper focuses only on the laptop use in planning a protest, in order to keep the example at a reasonable size.

Since the group is concerned about its IT Security, it consults security guidelines for activists to be found on the Internet. Three of these guidelines are examined:

- *A Practical Security Handbook for Activists and Campaigns* (ActivistSecurity.org Collective 2008)
- *Surveillance Self-Defense* by the Electronic Frontier Foundation (EFF n.d.)
- The *Security in-a-box website* (Tactical Technology Collective/Front Line Defenders n.d)

One of the most complete guidelines is *A Practical Security Handbook for Activists and Campaigns* (ActivistSecurity.org Collective 2008). The booklet gives a comprehensive view of activist security. Only the parts of the booklet dealing with data security for activists are of interest here.

The authors identify activist security mostly as an issue of information security: "On a practical level for campaigners and activists most security processes are essentially about controlling the flow of information about yourself and your plans, whether electronic, personal data, paper trails or physical evidence which connects you to the action" (ActivistSecurity.org Collective 2008: 4). The authors focus on confidentiality: "When you understand where there are potentially betraying information leaks out, you arrange to have the security techniques and processes to stem that flow, or at least make it very difficult for it to be traced" (ActivistSecurity.org Collective 2008: 4).

Chapter 6.2.3 of the Activist Security booklet addresses IT Security, namely securing phone calls, computers, and email (cf. Activist Security: 35). The booklet mostly gives advice regarding specific technology like Skype. It is concerned with confidentiality only.

Chapter 8 of the Activist Security booklet is dedicated to Computer Security and Internet Privacy. Here, the authors do not present a risk/threat analysis and jump straight into recommendations (cf. Activist Security: 56):

- Use Ubuntu/Debian Linux OS
- Use Firefox for web browsing
- Use Thunderbird for email
- Encrypt Email with Enigmail/GPG
- Use disk encryption
- Browse anonymously with TOR and FoxyProxy

The Activist Security booklet also has a section dedicated to Data Management (Chapter 8.3). The advice is (cf. Activist Security: 58f):

- Encrypt sensitive information with GPG or PGP
- Keep sensitive information on external storage
- Keep backups and store them not in your house
- Keep keys on memory stick
- Use dedicated wipe program for file deletion
- Use disk encryption
- Delete old data

The importance of threat modelling and finding suitable measures for a concrete threat model is mentioned several times in the Activist Security booklet, for example "There are pros and cons to using common freemail ones such as Hotmail, Yahoo as opposed to RiseUp.net, Resist.ca, etc. The former have the advantage of being anonymous by being buried among the vast numbers of other users but poorer security; the latter have better internal security but draw attention by being so associated with activism" (Activist Security: 12).

However, it does not become clear how the concrete measure above can be tailored for the concrete threats of a group. How to weight the pros and cons of using activist email-services like RiseUp.net compared to using common freemail services like Hotmail or Yahoo? Is email a suitable media for communication at all, or should other means of communication be selected? What consideration should be taken into account when deciding if the TOR anonymizing network should be used for browsing the web? In order to answer these questions, a detailed analysis of the threat landscape is required. For example, an adversary who is able to track all Internet surfing habits of group members may get insights into planned activities of the group if members surf the web non-anonymously. On the other hand, using the TOR anonymous network for web surfing increases the risk of active attacks, therefore extra caution is required.

Another guideline comes from the Electronic Frontier Foundation (EFF). The Electronic Frontier Foundation is probably the most renowned digital rights organization in the world. As part of their project *Surveillance Self-Defense* they provide a text named *Activist or Protestor?* (EFF 2015) with IT Security advice for activist. They identify the following fields requiring protection:

– Communicating with Others
– Keeping Your Data Safe
– Circumvent Online Censorship
– Attending Protests
– Protecting Yourself on Social Networks

In this paper, we only consider the first two points, 'Communicating with Others' and 'Keeping Your Data Safe'. 'Circumvent Online Censorship' and 'Protecting Yourself on Social Networks' are not part of the domain modelled. While 'Attending Protests' may seem relevant, for the example group this paper only focus on the communication aspect of planning the protest. It can be assigned to the basic principles of Confidentiality, Integrity, and Availability as follows:

– Communicating with Others (Confidentiality, Integrity, Availability)
  An activist will both be interested in the confidentiality of the conversation (keeping eavesdroppers out), as well as the integrity (she wants to be sure that neither her desired communication partner nor she herself can be impersonated by a third party), and availability (a third party should not be able to disrupt her communication infrastructure).
  The EFF only addresses the aspect of confidentiality in their guideline. The recommendation is to use end-to-end encryption. For email PGP[2] and TLS[3] are explicitly mentioned. They also point out that meta-data (who communicated with whom?) is not protected by these measures (EFF 2015).
– Keeping Your Data Safe (Confidentiality, Integrity, Availability)
  Again, both the Confidentiality, Integrity, and Availability may be threatened. Third parties should neither be able to get to know confidential data, nor should they be able to manipulate it or to prevent legitimate parties from using the data. Again, the EFF's guideline addresses confidentiality only.

They make the following recommendations (cf. EFF 2015):

– Use full-disk encryption for the computer hard disk (Bitlocker[4] if Windows, built-in encryption if Linux)

2 PGP (Pretty Good Privacy) was one of the first programs providing strong encryption for emails. Nowadays PGP typically refers not to the specific program PGP, but to the OpenPGP protocol and programs implementing it.

3 TLS (Transport Layer Security) was developed under the name SSL (Secure Socket Layer) for encryption of web traffic. Now TLS it is a protocol-agnostic standard for encryption of Internet traffic.

4 Bitlocker is a tool for disk encryption. It is part of the ultimate and enterprise versions of Microsoft Windows.

– Preferably, use Linux as an operating system
– Use strong passwords (over fifteen characters long)
– Keep/hide computer in a physical safe space, e.g. a locked cabinet
– Use separate machine of security-critical tasks
– Keep encrypted copy of data elsewhere
– Do not connect computer with critical data (e.g. encryption keys) to the Internet
– Use TOR
– Use dedicated insecure computer when going to dangerous places

Threat modelling is mentioned in the text. In fact, it starts with a chapter on threat modelling. In order to start threat modelling, they recommend answering the following questions (cf. EFF 2015):

1. What do you want to protect?
2. Who do you want to protect it from?
3. How likely is it that you will need to protect it?
4. How bad are the consequences if you fail?
5. How much trouble are you willing to go through in order to try to prevent those?

Threat modelling is also addressed in subsequent chapters, for example:

> "remember your threat model. You don't need to buy some expensive encrypted phone system that claims to be 'NSA-proof' if your biggest threat is physical surveillance from a private investigator with no access to internet surveillance tools. Alternatively, if you are facing a government that regularly jails dissidents because they use encryption tools, it may make sense to use simpler tricks — like a set of pre-arranged codes — rather than risk leaving evidence that you use encryption software on your laptop" (EFF 2015).

Like for the Activist Security booklet, the EFF's text does not provide advice on how to tailor the security recommendations to the specific threat model.

The *Security in-a-box* project is also a well-known resource for information on IT Security for activists. Besides concrete counter-measures to threats, it also gives information how to systematically model the threat landscape (cf. Tactical Technology Collective/Front Line Defenders n.d.). However, it does not tie the threat analysis to concrete countermeasures.

In summary, the exemplary activist group gets a number of concrete recommendations from the guidelines studied above. It is not always clear if these recommendations are applicable to their threat scenario: Shall they use Linux on all their laptops or is Windows acceptable? Should they use TOR to access their email? Do they have to lock away their computers when not in use? The *Security*

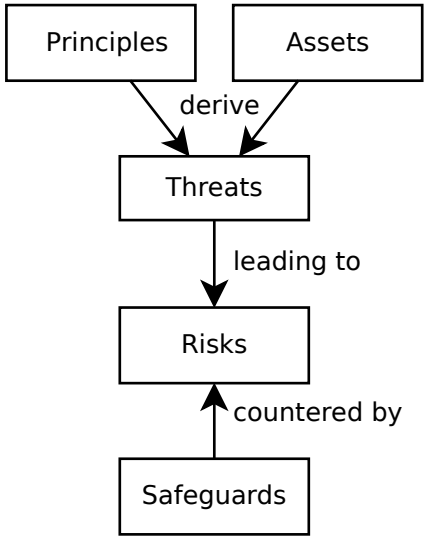
in-a-box project is one of the few security guidelines for activists providing in-depth information on threat modelling and risk analysis, but it does not link the threat analysis to concrete counter-measures.

4. Professional IT Security Modelling and Risk Analysis

4.1 The Security Modelling Process

In the previous chapter, we addressed the problem that our example group does not know which of the safeguards mentioned in the various guidelines are applicable to their specific situation, and if the recommendations given in these guidelines counter all relevant threats. We will now show how professional IT security modelling and risk analysis would approach this scenario. We show how the systematic methodology of IT security modelling and risk analysis is able to overcome the shortcomings of the ad hoc approaches.

Figure 1: Relationship between Threats, Risks, and Safeguards



The IT Security community agrees on the basic methodology of how to assess and improve IT Security: A security analysis starts by identifying the *assets* to be protected in respect to *basic principles*. These assets are endangered by *threats*. The security practitioner determines the *risk* that a *threat* is realized. Based on this *risk*, she determines whether the given state of protection is suitable or how it has to be adapted, for example by adding safeguards. See Figure 1.

For each of the assets, one collects how this asset has to be protected in respect to confidentiality, integrity and availability. Typically, these basic principles are always addressed in a security analysis. Even if some are deemed not relevant, this conclusion is the result of the security analysis. Depending on the concrete topic, more principles can be added, for example anonymity (the identity of the author must not be disclosed to third parties), non-repudiability (it is not possible to deny that a communication took place), etc.

Next, one identifies the threats to the assets. In case of assets to be protected in respect to confidentiality, threats are related to disclosure of information about the asset. In case assets have to be protected in respect to integrity, the threat is data manipulation. In regard to availability, the threat is making the asset unavailable.

The next step in an IT Security analysis is risk modelling. The severity of a risk depends on the damage caused if an asset is violated, and the likelihood that the corresponding threat is realized (cf. Courtney 1977). Consequences can range from mild to severe. For example, a mild consequence of a confidentiality violation could be an increased amount of spam due to public disclosure of one's email address. A severe consequence of a confidentiality violation could be threats to one's life because one's homosexuality becomes public.

The kind and severity of a threat may also depend on the threat agent, that is the person or organization responsible for the threat. Therefore identifying threat agents is important. For example, a threat on confidentiality by a marketing company, interested in collecting data for an advertisement campaign, is typically less severe than a threat posed by an intelligence agency.

4.2 Risk Assessment

There are different approaches to risk assessment. Since the process of IT risk assessment is typically conducted for company IT structures, risks are typically quantified in monetary terms. Risk is calculated as the product of the monetary damage when the threat is realized and the probability of the threat being realized. This already poses problems in a professional environment and even more so for a grass-root organization: Typically, both the probability of a threat being realized and the monetary damage if it is realized are rough estimates. These rough estimates are used to calculate numbers that appear accurate but are not more than rough estimates themselves. Sometimes, they are not applicable at all.

Therefore other approaches exist. A common approach is to categorize risks on an ordinal scale as 'normal', 'high', or 'very high' (cf. BSI 2008b: 47f). This approach raises the question how these categories are defined. In Germany, BSI (*Bundesamt für Sicherheit in der Informationstechnik* – Federal Office for Information Security) provides the *IT Grundschutz* (IT Basic Protection) framework in order to provide small and medium-sized business a framework to improve their IT security. As the name suggests, this framework provides means for basic protection, but certification according to the international standard ISO 27001 (ISO/IEC 27001 2011) is possible as well. *IT Grundschutz* uses three levels of risk, 'normal', 'high', and 'very high'. *IT Grundschutz* also provides suggestions on how to define these levels. For each level ('normal', 'high', and 'very high'), criteria in respect to the following six categories are given (BSI 2008b: 47f):

1. Violations of laws, regulations, or contracts
2. Impairment of the right to informational self-determination
3. Physical injury
4. Impaired ability to perform tasks
5. Negative internal or external effects
6. Financial consequences

For example, in respect to 'Impaired ability to perform tasks', the following criteria are given:

– Normal
  "Impairment was assessed to be tolerable by those concerned. The maximum acceptable downtime is greater than 24 hours" (BSI 2008b: 2).
– High
  "Impairment of the ability to perform the tasks at hand was assessed as intolerable by some of the individuals concerned. The maximum acceptable down time is between one and 24 hours" (BSI 2008b: 2).
– Very High
  "Impairment of the ability to perform tasks was assessed as intolerable by all individuals concerned. The maximum acceptable down time is less than one hour" (BSI 2008b: 2).

As one can already see, these criteria are not fully suitable for our environmentalist group and have to be adapted. Others are directly applicable to small groups and individuals, most notably items 2 ('Impairment of the right to informational self-determination') and item 3 ('Physical injury'), but also other items can be adapted easily, especially item 5 ('Negative internal or external effects') and 6 ('Financial consequences').

For example the group may consider the consequences if group membership or participation in an activity of the group becomes publicly known. Depending on the consequences, the protection requirements for confidentiality may be 'normal', 'high', or 'very high'. *IT Grundschutz* gives the following guidelines to determine these requirements. If the result of a disclosure "could adversely affect the social standing or financial well-being of those concerned", the protection requirement category is 'normal' (BSI 2008b: 48). If the consequences would be "seriously adverse affect on the social standing or financial well-being of those concerned", the category would be 'high' (BSI 2008b: 48). If the disclosure could result in "injury or death of the persons concerned or [...] could endanger the personal freedom", the category would be 'very high' (BSI 2008b: 49). Therefore confidentiality requirements could be classified as 'normal' in a liberal state, while they may rise to 'very high' in an authoritarian state.

4.3 Mitigating Risks

As a result of the security model, the IT Security professional has identified the risks to the assets. The next step is to address these risks. The literature identifies four strategies for dealing with risks (cf. Katsikas 2013: 913f):

– Avoid the risk
  One restructures one's activities in order to avoid a risk. The activist group may decide to switch to a field of politics where they are not subject of repression.[5]
– Reduce the risk
  As already described, risk can be measured by multiplying the likelihood that a threat is realized by the damage of the realization of the threat. This number can be reduced by reducing any of these factors. For example, the group may decide to improve their security standards for confidentiality by using encrypted email.
– Outsource the risk
  The risk is dealt with by delegating it to somebody else. For a political group, this could for example mean to enlist prominent public persons to public support their cause, thus drawing potential repression to persons who are better protected due to their popularity.
– Accepting the risk
  Finally, one can decide to accept a risk. This would be a very common strategy for a political group. The concept of 'civil disobedience' is based on incor-

5 This of course means to change their politics. This will be addressed in Chapter 6.

porating the repression resulting from realization of risks into a political strategy.

4.4 Safeguards

Where the risk reduction strategy is chosen, one has to identify appropriate safeguards. Typically, expert knowledge is required to identify or develop safeguards. However, there are also approaches suitable for non-experts. *IT Grundschutz* provides a set of catalogues of modules for the typical IT infrastructure of a small to medium-sized company (cf. BSI 2013). These modules are cross-referenced with typical threats to these modules and suitable safeguards. It explicitly provides safeguards for security requirements level 'normal' only. For those items with higher security requirements, the practitioner may have to develop his or her own safeguards. *IT Grundschutz* also provides guidance for this.

4.5 Model based on IT Grundschutz

Next, the example scenario is modelled according to *IT Grundschutz*. In regard to planning an action, the group's security guideline is that information both about the plan and the participants should remain confidential. Furthermore, communication within the group should always be possible. Confidentiality of membership and the availability of communication should be maintained but is not critical. On the other hand, confidentiality of the communication is of critical importance. These requirements are summarized in Table 1.

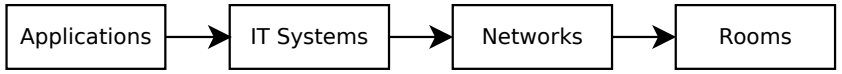
Table 1: Protection Requirements

Processes	*Confidentiality*	*Integrity*	*Availability*
Protest planning	Normal	n/a	n/a
Participating in Protest	Normal	n/a	n/a
Group Membership	Normal	n/a	n/a
Group Communication	High	n/a	Normal

Following the *IT Grundschutz* methodology, one first identifies the relevant processes to protect. A number of processes have been identified in Table 1. For brevity we only consider protest planning by email.

IT Grundschutz continues by identifying the IT equipment, communication links, and rooms used for the applications (cf. Figure 2). The group uses

Figure 2: IT Grundschutz Process



laptop or desktop PCs on the Internet for communication. Since the group is heterogeneous, no further assumptions are made: Some computers may be stationary PCs in an apartment, protected by the router/firewall of the local network, others may be laptops used on a public wifi access point with no further protection at all.

In the next step, protection requirements are defined. In our example, we require high protection in respect to confidentiality, and normal protection in respect to availability. This categorization is transitively applied to the network(s), computer system(s), and room(s) involved.

After the protection requirements have been determined, *IT Grundschutz* catalogues list threats and safeguards for the objects to be protected. Besides the four aspects addressed above, applications, networks, IT systems and infrastructure (rooms), there is a fifth category, common aspects. These are security considerations not bound to specific processes (cf. BSI 2013: 42ff). In order to keep our example small, we will not go into details.

From the list given in the catalogues, the modules 'M 5.3 Groupware' and 'M 5.8 Telecommuting' are relevant for our example application. 'M 5.3 Groupware' covers collaboration of working groups using IT systems. It is relevant, because it includes collaboration by email. 'M 5.8 Telecommuting' is relevant, because it addresses work out-of-office (which is the case for everybody in our environmentalist group, because the group does not have an office). For brevity we only look at threats for 'M 5.8 Telecommuting'. *IT Grundschutz* Catalogues organizes threats according to the categories 'Force Majeure', 'Organisational Shortcomings', 'Human Error', 'Technical Failure', and 'Deliberate Acts'. The list for Deliberate Acts contains for this module contains:

"– T 5.1 Manipulation or destruction of equipment or accessories
– T 5.2 Manipulation of information or software
– T 5.9 Unauthorised use of IT systems
– T 5.10 Abuse of remote maintenance ports
– T 5.18 Systematic trying-out of passwords
– T 5.19 Abuse of user rights
– T 5.20 Misuse of administrator rights
– T 5.21 Trojan horses
– T 5.71 Loss of confidentiality of classified information" (BSI 2013: 354)

In order to counter the threats, the catalogues provide safeguards. The categories of safeguards for a given object correspond to the life phases of the object:
– Planning and design
– Implementation
– Operation
– Contingency Planning

For the planning phase, the following safeguards are listed:

"– S 2.113 (A) Requirements documents concerning telecommuting
– S 2.114 (A) Flow of information between the telecommuter and the institution
– S 2.115 (B) Care and maintenance of workstations for telecommuting
– S 2.116 (A) Regulated use of telecommuting communication capabilities
– S 2.117 (A) Creating a security concept for telecommuting
– S 2.205 (C) Transmission and retrieval of personal data
– S 2.241 (C) Procedure for carrying out a teleworkstation requirements analysis" (BSI 2013: 356).

Some of these safeguards are not applicable outside of a company environment. For example S 2.113 (Requirements documents concerning telecommuting) addresses "issues relating to labour regulations and occupational safety laws need to be taken into account when designing the telecommuting framework" (BSI 2013: 1470). Others are highly relevant, like S 2.115, which addresses the need to define how maintenance of the group's laptops is carried out, and S 2.117, which demands the creation of a security concept for using the laptops.

For the remaining phases, the following safeguards are provided:

"– Implementation
  (a) S 4.63 (A) Security-related requirements for telecommuting computers
  (b) S 5.51 (A) Security-related requirements for communications links between telecommuting workstations and the institution
  (c) S 5.52 (A) Security-related requirements for communications computers
– Operation
  (a) S 3.21 (A) Training of telecommuters as regards (in puncto) security-related issues
– Contingency Planning
  (a) S 6.47 (B) Storage of backup copies as part of telecommuting" (BSI 2013: 356).

For each of these safeguards, the *IT Grundschutz* catalogues gives extensive advice. For example, 'S 4.63 Security-related requirements' for telecommuting computers spans 4 pages, and addresses (among other aspects) identification and authentication mechanism, access control mechanism, backing up data, encryption, boot protection mechanism, and computer virus scanning programs (cf. BSI 2013: 2719ff).

Regarding the rooms, the *IT Grundschutz* modules M '2.8 (Home workplace)' and 'M 2.10 (Mobile workplace)' are applicable. For 'M 2.8 (Home workplace)', one of the threats is 'T 2.6 (Unauthorised admission to rooms requiring protection)'. A safeguard is 'S 1.19 (Z) (Protection against entering and breaking)', requiring hardening the room against burglars, including:

"– Using burglar-resistant doors and windows [...]
– Using roller shutter locks on doors or windows that could be used to break in to the building,
– Using special lock cylinders, additional locks and bars" (BSI 2013: 1168).

In the same way, guidance for all safeguards is provided. By systematically evaluating the threats and safeguards for all assets, the group gets guidelines on how to protect their assets.

The safeguards provided in the *IT Grundschutz* catalogues are sufficient to protect assets with security requirements of 'normal'. For the advanced level 'high' and 'very high', an enhanced security analysis is required in order to determine if the *IT Grundschutz* safeguards are sufficient.

Further analysis reveals that for the group of activists, S. 1.19 may not be sufficient to protect the home workspace. While the safeguards may be sufficient for profit-oriented burglars, they are not sufficient for state sponsored burglars, i.e. police or intelligence agencies. Further considerations reveal that it is nearly impossible to come up with improved safeguards for this scenario. The activist group has to re-evaluate their use of communication equipment in a risk analysis. Considering the risk mitigation strategies from Chapter 4.3, the group comes to the conclusion that neither accepting nor outsourcing the risk is an option. Reducing the risk is beyond the groups capabilities. Therefore the group decides to avoid the risk by having physical meetings for organizing the protest instead of using email.

5. Comparison of The Security Analysis with Security Guidelines

A systematic approach to threat analysis and modelling as described for example in the *IT Grundschutz* methodology augments hands-on guidelines by allowing the practitioner to determine which safeguards from the guidelines are to be applied, and which further safeguards may be necessary. In our example, it turned out that the safeguards provided in the guidelines are not sufficient. The risk of physical

manipulations of IT equipment, which is possible because our small activist group is not able to protect the rooms where their laptops are used, is underestimated.

Risk analysis and mitigation strategies also provide guidelines to alternative risk mitigation strategies besides improving the safeguards. In our example, an alternative strategy – in-person meetings – was agreed upon. This shows that risk mitigation strategies come at a price: Reducing a risk by improving safeguards may cost time, money and effort. It also may make the actual process/application harder to conduct. Avoiding a risk may mean to cease activities and alter one's behaviour. It should be noted that the very serious danger that risk mitigation strategy turn counter-productive is addressed in the guidelines analysed for this paper. For example, the Riseup booklet states: "People and groups get so tied up in making sure their action is secure that they end up not doing the action, or they only do it in a very tiny way with a very tiny group of trusted friends. When security culture makes us too paranoid to publicize any kind of action, our activist priorities have been turned backwards" (The Riseup Collective n.d.: 5).

6. Conclusion

Most approaches of professional IT Security Engineering boil down to risk assessment based on monetary values: Risk is (directly or indirectly) measured by multiplying the monetary damage if a risk is realized by the likelihood of the risk being realized. If taking the risk is not economically viable, the business is adapted or more viable lines of business are explored. A common critique of this approach is that often measuring risk in terms of monetary value is not possible due to lack of information about (potential) damage or inappropriateness of measuring risk as monetary values (for example because human life is at stake). This line of reasoning applies even more to groups that are not economically motivated, like the environmentalist group used as an example.

When economically viability is not the prime motivation, the methods of dealing with risks warrant further investigation. For a company, the ultimate goal is to make a profit. Therefore it makes perfectly sense to pull out of a business because the risk becomes too high, that is a negative profit is to be expected due to a high risk. For groups who are not primarily motivated by profit – or even aim at transcending capitalism – this kind of risk assessment does not always make sense. The strategies for dealing with risk described in the previous chapters are not always applicable: Reducing a risk by increased security measures may be counter-productive, because the group becomes less accessible. Outsourcing risk does not fit the agenda of a grass-root organization. Avoiding a risk may mean to surrender to the political opponent. On the other hand, the rigorous approach to threat and risk analysis of professional IT Security methodologies allows better insights into identifying threats to individuals and small groups. Since many threats to these targets are directly related to IT Security/the processing of personal data, standard IT Security methods can be applied to counter these threats.

It has been shown how activist security guides reflect the approaches of professional security management methodologies. While guidelines for activists on IT Security are clearly influenced by professional IT Security management approaches, they do not fully follow the systematic approach of professional IT Security modelling. The small example of the environmentalist group showed that using professional approaches allows activists to come up with sound security designs. However, professional security methodologies are tailored for companies and large organizations. Industrial standards for IT security – even the ones adaptable for small companies and organizations like BSI's *IT Grundschutz* – are typically too big for small groups. Further research should address the following questions:

- How does the security landscape change when the adversary is a state (-sponsored) organization?
- How can existing security management methodologies be adapted for small groups and organizations?
- What are the adversary effects of risk mitigation strategies on the goals processes, and applications of individuals and activist groups?

Bibliography

ActivistSecurity.org Collective (2008): A Practical Security Handbook for Activists and Campaigns. Version 2.7. URL: http://www.activistsecurity.org/booklet-2.7%28final%29.pdf [19.10.2105].

BSI (2008a): BSI-Standard 100-1 – Information Security Management Systems (ISMS). Version 1.5. Bonn. URL: https://www.bsi.bund.de/SharedDocs/Downloads/EN/BSI/Publications/BSIStandards/standard_100-1_e_pdf.pdf?__blob=publicationFile [12.11.2015].

BSI (2008b): BSI-Standard 100-2 – BSI-Standard 100-2: IT-Grundschutz Methodology. Version 2.0. Bonn. URL: https://www.bsi.bund.de/SharedDocs/Downloads/EN/BSI/Publications/BSIStandards/standard_100-2_e_pdf.pdf?__blob=publicationFile [12.11.2015].

BSI (2013): IT-Grundschutz-Catalogues. Version 13. Bonn. URL: https://gsb.download.bva.bund.de/BSI/ITGSKEN/IT-GSK-13-EL-en-all_v940.pdf [12.11.2015].

Courtney, Robert H, Jr. (1977): Security risk assessment in electronic data processing systems. In: AFIPS Conference Proceedings of the National Computer Con-

ference 46. ACM New York. URL: https://www.computer.org/csdl/proceedings/afips/1977/5085/00/50850097.pdf [12.11.2015].

EFF (n.d.): Surveillance Self-Defense. URL: https://ssd.eff.org/ [12.11.2015].

EFF (2015): Activist or protester? – How to keep you and your communications safe wherever your campaigning takes you. URL: https://ssd.eff.org/en/playlist/activist-or-protester [12.11.2015].

Ellis, Scott R. (2013): Fundamentals of Cryptography. In: Vacca, John R. (ed.): Computer and Information Security Handbook. Waltham. 1031-1038.

ISO/IEC 27001 (2011): Information technology – Security techniques – Specification for an Information Security Management System. Geneva.

Katsikas, Sokratis K. (2013): Risk Management. In: Vacca, John R. (ed.): Computer and Information Security Handbook. Waltham, MA, USA: Morgan Kaufmann. 905-927.

Pfleeger, Charles P., Pfleeger, Shari Lawrence (2007): Security in Computing. Fourth Edition. Boston.

The Riseup Collective (n.d): Digital Security for Activists. URL: https://zine.riseup.net/assets/digital_security_for_activists.pdf [12.11.2015].

Stallings, William; Brown, Lawrie (2012): Computer Security – Principles and Practice. Second International Edition. Harlow.

Tactical Technology Collective, Front Line Defenders (n.d.): How to assess your digital security risk. URL: https://securityinabox.org/en/lgbti-africa/security-risk [12.11.2015].

WESTFÄLISCHES DAMPFBOOT
E-Mail: info@dampfboot-verlag.de
http://www.dampfboot-verlag.de