Chapter 8
Risk Analysis

Having identified cyber-threats, vulnerabilities, and the incidents that constitute risks by harming the identified assets, our next task is to assess the likelihood of these incidents and their consequence for each of the affected assets, so that the risk level can be determined. In order to achieve this, it is usually necessary to perform an analysis of the related threats and vulnerabilities. This also helps us to better understand what contributes to the risk, which is useful for identifying treatments.

As illustrated by Fig. 8.1, we analyze the likelihood for threats to materialize in terms of the frequency scale defined during the context establishment. For severity of vulnerabilities we prefer to use a simple scale consisting of the steps *High*, *Medium*, and *Low*, as the severity cannot be directly captured by frequencies. Finally we analyze the likelihoods and consequences of incidents in terms of the scales defined during the context establishment. The information sources we exploit for the risk analysis are more or less the same as those used for risk identification. The main difference is that now we also need to consider the severity of vulnerabilities and the likelihood of threats and incidents, as well as the consequence of incidents, rather than simply determining whether the threats, vulnerabilities, and incidents are relevant or not. In the following we demonstrate the reasoning behind the analysis for some selected examples. When documenting the risk assessment we make sure to include all the information sources and reasoning behind the analysis, typically in an appendix to the risk assessment report.

8.1 Threat Analysis

We start the risk analysis by analyzing threats. Due to their different nature, it is normally useful to look at malicious and non-malicious threats separately, which is what we do below. However, the distinction is not always clear-cut, and some threats may be both malicious and non-malicious. In such a case, we usually prefer to include it among the malicious threats. However, the important thing is that the threat is not left out and that both its malicious and non-malicious aspects are considered.

A. Refsdal et al., *Cyber-Risk Management*, SpringerBriefs
in Computer Science, DOI 10.1007/978-3-319-23570-7_8

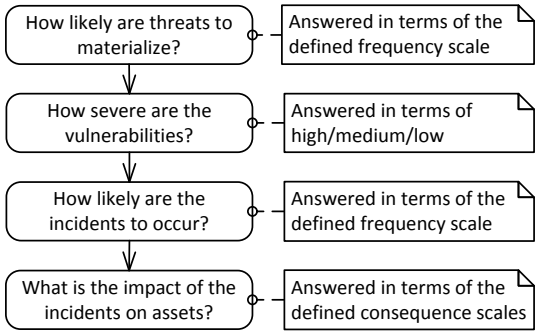

Fig. 8.1 Overview of risk analysis process for our smart grid risk assessment

8.1.1 Malicious Threats

We start by analyzing the threat *DDoS attack on the central system* from Table 7.3. Our main sources of information in estimating its likelihood are the event logs provided by the distribution system operator, as well as the expert judgments of the participants. We choose to follow an approach inspired by the OWASP risk-rating method [62], which uses the threat source factors of skill level, motive, opportunity, and size to analyze the threat. The factors are rated on a scale from 0 to 9.

As the first step in analyzing the threat of a DDoS attack, we consider the threat source. In this case we have actually identified two different threat sources, a script kiddie and a cyber-terrorist. We therefore look at each of them in turn.

Table 7.2 tells us that the script kiddie is relatively unskilled and unable to perform complicated attacks. We therefore assign skill rating 3. We have no reason to believe that script kiddies have specific interest in this particular power distribution system, but we know they are sometimes attracted to critical infrastructures in general. The motive for conducting a specific attack is also generally weak, so for this we assign rating 1. The opportunity is a measure of the resources and opportunities that the script kiddie requires to conduct the attack, for which we assign rating 7. Finally, size is a measure of how large this group of threat sources is. As script kiddies can reside anywhere in the world, we assign the rating 7.

For the cyber-terrorist, we again consult Table 7.2. Based on the description there, we assign skill level 7, motive 8, and opportunity 7. Since we assume that the number of cyber-terrorists is much lower than that of script kiddies, we assign a size rating of 3, even if cyber-terrorists may also reside anywhere in the world.

The OWASP method prescribes taking the average of the threat source factors to obtain an overall rating for the threat. For the script kiddie, the average equals 4.5. For the cyber-terrorist, the average equals 6.25. This means that the threat level is quite high. Based on these results and using our own likelihood scale defined in Table 6.3, we estimate the likelihood of this threat to be *Likely*, as documented in Table 8.1. At this point, you should always check that the estimate is supported by the available event logs and confirmed by the participants from the distribution system operator. We follow a similar approach for the remaining malicious threats.

Table 8.1 Malicious threat analysis

Threat	**Likelihood**	Estimate basis/comments
DDoS attack on the central system	Likely	This kind of attack is frequent and requires modest skills and resources. The estimate is confirmed by event logs and by cybersecurity statistics
Tampering with all or most control data in transit from the central system to the choke component	Possible	Dedicated cyber-terrorists are probably able to perform such attacks. Although few instances have been recorded so far, reports from Interpol and similar agencies give reason to expect increased likelihood of this type of attack
Tampering with data in transit from the metering terminal to the central system	Possible	Complaints from electricity customers and subsequent investigations indicate that this kind of tampering has occurred in recent years, although the number of incidents and affected customers is hard to estimate
Malware to manipulate meter data is installed on the metering terminal through connection to the external meter	Possible	Tests have revealed that such an attack is technically not very difficult, but it requires access to the connection to the external meter. Although the number of incidents may be fairly high, the number of affected meters will therefore be small
Metering node infected by malware	Rare	Although the metering node is connected to the Internet, it is quite different from standard computers, and does not run most of the software targeted by most malware
Tampering with control data in transit from the central system to the choke components for selected electricity customers	Unlikely	Such threats have not yet been observed by the central system operator. However, recent developments may indicate that activists are increasingly willing to target political adversaries in this way
Illegitimate control data sent to the choke components from the central system	Unlikely	The central system operator has not experienced any such instances, but this has happened in other companies. Employee satisfaction surveys indicate that the central system operator employees are loyal. However, if an insider actually wants to perform such an attack, she is likely to succeed

8.1.2 Non-malicious Threats

Non-malicious threats are by nature unexpected or unintended events that happen by accident or by chance. In analyzing such threats we also start by considering the threat source. By understanding who or what may cause the threat, we can better understand how likely the threat is to occur. Further sources of information include event logs, expert judgments, interviews or questionnaires, and available statistics about the typical likelihood of similar threats in enterprises and other organizations. For the analysis of non-malicious threats we need to keep in mind that threats and

near incidents that have occurred before may not be reported or registered. This can, for example, be due to lack of reporting routines and due to the reluctance of personnel to do self-reporting. To establish a better basis for the analysis of non-malicious threats we can investigate relevant properties of the organization, such as culture, routines, skills, security awareness, procedures, and so forth.

For the threat *Mistakes during update/maintenance of the central system* from Table 7.9, for example, we first consider the threat source, namely the *Maintenance personnel*. By identifying who they are and what their responsibilities and job tasks are, we get an understanding of how and when they can cause the identified threat. In addition to this we may base our estimate on the event log and on the judgment made by, for example, the head of the maintenance team. There is evidence that mistakes are made on an almost monthly basis on average, as documented in Table 8.2 by the estimate *Certain*. Notice that at this point we estimate the likelihood of any mistake, no matter how grave. We follow a similar approach for the remaining non-malicious threats.

Table 8.2 Non-malicious threat analysis

Threat	**Likelihood**	Estimate basis/comments
Internet connection to the metering terminal goes down	Certain	This includes cases where individual electricity customer's homes lose Internet connection, which according to general statistics happens very often
Buggy software distributed on metering terminals	Possible	This estimate is based on patching logs for various software products developed by the provider of metering terminal software during the last four years
Mistakes during update/maintenance of the central system	Certain	This estimate is based on event logs and statements from the head of the management team
Electricity customer home/building is struck by lightning	Certain	This estimate is based on statistics for the geographical area where the electricity customers are located

8.2 Vulnerability Analysis

The next step consists of analyzing vulnerabilities. For this we choose to use a simple scale consisting of the steps *High*, *Medium*, and *Low*. Again we distinguish between vulnerabilities with respect to malicious and non-malicious threats.

8.2.1 Malicious Threat Vulnerabilities

For the assessment of the severity of the identified vulnerabilities we can again make use of the information sources of expert judgments, statistics, and open repositories. But we can also investigate our target of assessment by conducting, for example, vulnerability scans, security testing, penetration testing, and code review.

The identified vulnerability regarding the DDoS attack according to Table 7.4 is *Inadequate attack detection and response on central system*. Inspired by the OWASP risk-rating method we rate vulnerabilities by using the factors of ease of discovery, ease of exploit, awareness, and intrusion detection.

The ease of discovery is a measure of how easy it is for the possible threat sources to come upon this vulnerability. Checking whether systems are vulnerable to DDoS attacks is often straightforward, and we therefore assign the value 7 (easy) to this factor. For the ease of exploit we need to investigate the target of assessment, and perhaps conduct some testing. Already during the risk identification we ascertained that this is a vulnerability that obviously can be exploited. Security testing can confirm this by demonstrating that most illegitimate requests are indeed not detected. For this reason we assign the rating 5 (easy) for the ease of exploit factor. The awareness factor is a measure of how well known this vulnerability is to the threat sources in question. As the knowledge of the existence of such vulnerabilities is widespread we assign the value 6 (obvious) to this factor. Similarly to the ease of exploit, we have already established that the intrusion detection is rather weak, partly based on insights from the experts and partly based on results from security testing. We assign the value 7 to this factor, meaning that intrusions are usually not detected when they happen. This leaves us with an average vulnerability score of 6.25. We consider 6.25 out of 9 to be quite severe, and therefore assign severity *High*, as documented in Table 8.3. We complete the table following a similar approach.

8.2.2 Non-malicious Threat Vulnerabilities

For the non-malicious threats there is of course no intent to discover and exploit vulnerabilities. Instead we seek to understand the extent to which there is a lack of barriers that could prevent threats from leading to incidents.

For the incidents resulting from the threat *Mistakes during update/maintenance of the central system*, for example, we identified the vulnerability *Poor training and heavy workload*, as shown by Table 7.8. After investigating the background and expertise of the maintenance personnel, looking into the tasks and routines, and interacting with the head of the maintenance team we may for example establish that the staff has strong training and expertise in system development. The security awareness, however, may be somewhat weak among some of the personnel, and we may also find that the workload during some periods is very heavy, at least for key personnel. At the same time, the routines for reviewing updates and testing the system before launching the updates are strong and thorough. Overall, our estimate

Table 8.3 Vulnerability analysis with respect to malicious threats

Vulnerability	**Severity**	Explanation
Inadequate attack detection and response on central system	High	Tests revealed that the DDoS attack detection mechanism is unlikely to detect a large part of illegitimate traffic. The response is based purely on dropping packets, which leaves little possibility of analyzing attacks
Weak encryption and integrity check	Medium	Inspections revealed that a weak encryption scheme is used for the data exchanged between the metering terminals and the central system. The same applies to the integrity checking
Unprotected local network, no sanitation of input data from the external meter	Medium	The central system operator has no control of the local networks of electricity customers. We must therefore assume that such networks may be poorly protected. There is no sanitation of input data from external meters to the metering terminals
Outdated antivirus protection on metering node	High	The antivirus protection on metering nodes is rarely updated
Four-eyes principle not implemented, no logging of actions of individual central system operators	High	Inspection of policies and interviews revealed that all tasks can be performed by a single operator. Moreover, the actions of individual operators on the central system are not logged

of the severity of the vulnerability in question is therefore *Medium*, as documented in Table 8.4. The remaining vulnerabilities have been addressed in a similar manner.

8.3 Likelihood of Incidents

In order to obtain an initial estimate of the likelihood of the incidents we consider the analysis of threats that lead to the incidents and the vulnerabilities that the threats exploit.

The incident *Data from metering nodes cannot be received by the central system due to DDoS attack* from Table 7.5, for example, is due to the threat *DDoS attack on the central system* and the vulnerability *Inadequate attack detection and response on central system*. For the threat we assigned likelihood *Likely*. The vulnerability severity was set to *High*, indicating that a large portion of the threat occurrences will actually lead to the incident. Although the number of DDoS attacks that succeed will likely be lower than the number of attempts, we still estimate that the frequency for the incident also lies within the interval of *Likely* on our scale. We retain this estimate even though event logs show only two such incidents for the last three years (which corresponds to *Possible*). This is because the threat and vulnerability analysis, supported by recent reports documenting increasingly advanced DDoS attacks on critical infrastructure, give good reasons to believe the frequency will increase

Table 8.4 Vulnerability analysis with respect to non-malicious threats

Vulnerability	**Severity**	Explanation
Single communication channel between central system and metering terminal	High	The Internet connection is the only communication channel to the central system for many electricity customers
Poor testing	Medium	Inspection of maintenance logs revealed a number of instances where bugs have been discovered in the metering terminal software. Previous experience indicates that the testing routines of the external software provider are unsatisfactory, and the central system operator does not test software updates for metering terminals before deployment
Poor training and heavy workload	Medium	Interviews indicate that security awareness is not high. Key persons have too much to do. Routines for reviewing and testing updates to the central system before deployment are strong
Inadequate overvoltage protection	High	The computing hardware of metering terminals is not robust with respect to transient overvoltage

compared to previous years. The result is documented in Table 8.5, which includes likelihood as well as consequence estimates for all malicious incidents.

To estimate the likelihood of the incidents that are caused by non-malicious threats, we also make use of the results of the analysis of threats and vulnerabilities. For example, the two incidents *Mistakes during maintenance of the central system disrupt control signals to the choke component* and *Mistakes during maintenance of the central system prevent reception of data from metering nodes* are caused by the same threat, as shown by Table 7.9. We estimated that the likelihood of the threat *Mistakes during update/maintenance of the central system* is *Certain*, and that the severity of the relevant vulnerability, namely *Poor training and heavy workload*, is *Medium*. At first glance this could be taken to imply that the two incidents occur with the same frequency. However, we found before that there are routines in place for reviewing and testing the system before changes are launched. Because provisioning of power to the electricity customer is more critical than the continuous reading of meter data, the routines are stronger with respect to updates and changes that may affect control data. This observation, combined with the data logs, leads us to the likelihood *Unlikely* regarding control data to the choke component, and the likelihood *Possible* regarding the reception of meter data. These estimates, together with the likelihoods and consequences for the other non-malicious incidents, are documented in Table 8.6.

8.4 Consequence of Incidents

The consequence of an incident must be judged for each asset it harms. For the incident *Data from metering nodes cannot be received by the central system due to DDoS attack*, for example, we need to estimate the consequence for the asset *Availability of meter data* according to the scale defined in Table 6.5. Therefore we need to consider the expected time it takes to detect and respond to an attack, as well as the number of affected electricity customers. In the experience of the distribution system operator, which is supported by their internal investigation reports of the incidents, the DDoS attacks that have occurred before have never caused loss of availability for more than one day. The number of electricity customers whose meter data becomes unavailable can, however, be higher than before, as the customer base has increased. Based on this information we therefore assign the consequence estimate *Moderate* to the incident in question, as documented in Table 8.5, which includes the estimates for all incidents resulting from malicious threat sources.

The provisioning of power to electricity customers is more critical than the availability of the meter data. This is also reflected by the consequence scales for the respective assets. This explains the consequence *Moderate* regarding the choke component (risk no. 14) and the consequence *Minor* regarding the meter data (risk no. 15), as documented in Table 8.6, which also includes the likelihood and consequence estimates for the remaining non-malicious incidents.

Table 8.5 Likelihood and consequence for incidents caused by malicious threats

No.	Incident	Asset	Likelihood	Consequence
1	Data from metering nodes cannot be received by the central system due to DDoS attack	Availability of meter data	Likely	Moderate
2	False control data received by all or most choke components	Provisioning of power to electricity customers	Unlikely	Critical
3	False meter data for a limited number of electricity customers received by the central system	Integrity of meter data	Likely	Minor
4	Malware compromises meter data	Integrity of meter data	Rare	Moderate
5	Malware disrupts transmission of meter data	Availability of meter data	Rare	Moderate
6	Malware disrupts the choke functionality	Provisioning of power to electricity customers	Rare	Major
7	False control data received by the choke components for selected electricity customers	Provisioning of power to electricity customers	Rare	Insignificant
8	Power supply to electricity customers is switched off without legitimate reason	Provisioning of power to electricity customers	Unlikely	Moderate

Table 8.6 Likelihood and consequence for incidents caused by non-malicious threats

No.	Incident	Asset	Likelihood	Consequence
9	Communication between the central system and the metering terminal is lost	Provisioning of power to electricity customers	Certain	Minor
10	Same as the row above	Availability of meter data	Certain	Insignificant
11	Software bug on the metering terminal compromises meter data	Integrity of meter data	Unlikely	Moderate
12	Software bug on the metering terminal disrupts transmission of meter data	Availability of meter data	Unlikely	Moderate
13	Software bug on the metering terminal disrupts the choke functionality	Provisioning of power to electricity customers	Rare	Major
14	Mistakes during maintenance of the central system disrupt transmission of control data to the choke component	Provisioning of power to electricity customers	Unlikely	Moderate
15	Mistakes during maintenance of the central system prevent reception of data from metering nodes	Availability of meter data	Possible	Minor
16	The metering terminal goes down due to damage from lightning	Provisioning of power to electricity customers	Likely	Insignificant
17	Same as the row above	Availability of meter data	Likely	Insignificant

8.5 Further Reading

For analyzing threats there are a number of sources and methods available. In addition to those provided by OWASP [62], there is the CAPEC catalogue offered by MITRE [51]. This gives ratings of attack prerequisites, attacker skills or knowledge, required resources, and attack indicator/warning. The CWE catalogue [52] also gives useful input for analysis of vulnerabilities.