Cybersecurity Ontology for Critical Infrastructures

Sandra Bergner and Ulrike Lechner
Fakultät für Informatik, Universität der Bundeswehr München, Germany

Keywords: Knowledge Engineering, Ontology Engineering, IT-Security, Critical Infrastructure.

Abstract: The number and frequency of hacker attacks on critical infrastructures like waterworks, government institutions, airports increase. The Cybersecurity of critical infrastructure is a complex topic with. A plenthora of requirements, measures from the BSI and the NIST as well as vulnerabilities that needs to be considered. This paper describes the ontology for IT-Security of critical infrastructures that combines the aforementioned requirements to give critical infrastructures a kind of guideline or roadmap for security and safety measures in order to preventively protect critical infrastructures of hacker attacks.

1 INTRODUCTION

The BMBF research program 'IT-Security for critical infrastructures' has been initiated as part of "Strategy 2020" of the German Government. Project VeSiKi 'Networked IT-Security of critical infrastructures' coordinates 13 research projects in the cooperative research process in the ITS|KRITIS initiative (www.itskritis.de) and (Bergner 2015a).

Project VeSiKi provides an ontology for IT- Security for critical infrastructures. The main goal of this ontology for IT-Security of critical infrastructure is to define a well-structured knowledge base for the topic itself and the 13 research projects of ITS|KRITIS, which design IT-Security technologies and which each have partners from various critical infrastructure sectors.

The ontology from Fenz (Fenz and Ekelhart, 2009) is considered state-of-the-art and offers a common basis with regard to IT-Security. However, this ontology does not take critical infrastructures into account. A second IT-Security ontology is the one of Tsoumas (Tsoumas and Grizalis, 2006).

We build on the seminal ontology of Fenz (Fenz and Ekelhart, 2009) as the basis Cybersecurity knowledge base. We enhance the Fenz ontology with knowledge from the Kaspersky Security list (Kaspersky, 2016) which includes information of current threats. We extend the Cybersecurity knowledge base with concepts derived from requirements from a critical infrastructure comitee like from the Bundesamt für Sicherheit in der Informationstechnologie (BSI) (BSI, 2013), vulnerabilities like from the National Vulnerability Database (NIST, 2016). We use the Miniduke malware as example for our models.

This paper introduces the ontology cybersecurity of critical infrastructures in its current development status. The ontology integrates subontologies in form of terminological knowledge (TBox concepts) to build up the models. In this paper we will introduce only parts of our ontology and present only the most relevant TBox concepts in detail.

Projects contribute assertational knowledge in form of ABox instances according to the specified TBox concepts. Thus, the subontologies (TBox and ABox) together build up a common knowledge base for the project teams of research institutions and providers of critical infrastructures. Hence, the main purpose is to establish an ontology which builds up the common knowledge base for an underlying dynamic knowledge pool for IT-Security of critical infrastructures.

The ontology is modelled in TopBraid ME Composer (https://www.topquadrant.com) in the modelling language OWL. The ontology has 95 classes and 1100 instances.

2 CYBERSECURITY ONTOLOGY

Four subontologies structure the common knowledge base: IT-Security, Project, Critical Infrastructure (CRITIS) and Compliance.

2.1 IT-Security Ontology

The IT-Security subontology covers the IT-Security

Bergner S. and Lechner U.
Cybersecurity Ontology for Critical Infrastructures.
DOI: 10.5220/0006510400800085
In *Proceedings of the 9th International Joint Conference on Knowledge Discovery, Knowledge Engineering and Knowledge Management (KEOD 2017)*, pages 80-85
ISBN: 978-989-758-272-1

relevant aspects like threats, controls and vulnerabilities. It is linked to the critical infrastructure (CRITIS) subontology and consequently to the appropriate assets of an organization.

2.1.1 IT-Security: TBox Concepts

The TBox concepts of the subontology IT-Security are based on the National Institute of Standards and Technology (NIST) NIST computer security handbook, NIST information security risk management guide (Stonebumer, Gary et al., 2002), ISO 27001 (ISO, 2013), German IT Grundschutz Manual BSI, 2013). It extends the Fenz ontology.

Figure 1 provides an overview of the IT-Security ontology TBox concepts. The TBoxes depicted in grey come from the Fenz ontology and are enhanced on the information from the Kaspersky web page (Kaspersky, 2016) as well as links to the VeSiKi projects which are TBoxes depicted in blue.

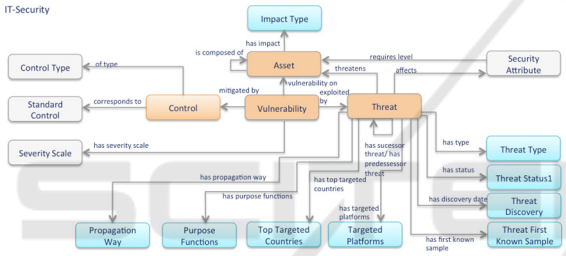

Figure 1: IT-Security Subontology TBox Concepts.

The IT-Security subontology is linked to the Critical Infrastructure Ontology (CRITIS) subontology and consequently to the assets of an organization.
The TBox-concepts Asset, Vulnerability, Control and Threat build up the core concepts of the Cybersecurity subontology and are depicted in orange:

- According to (ENISA, 2016) an Asset is defined as follows: “Anything that has value to the organization, its business operations and their continuity, including Information resources that support the organization's mission”.
- Each Asset concept (IT-Security: Asset ⊑ T) has an impact type(s), like
  (1) Allows unauthorized disclosure of information,
  (2) Allows unauthorized modification,
  (3) Allows disruption of service, etc. which might be again the Target Impact Type of the concept Threat.
- The concept Security Attribute (e.g. confidentiality, accountability, availability, integrity, reliability, or safety) defines the required level of the Asset and which Security Attribute might be affected by a certain threat accordingly.
- According to ENISA (ENISA, 2016), a vulnerability is defined as: „The existence of a weakness, design, or implementation error that can lead to an unexpected, undesirable event“. The Vulnerability concept (IT-Security: Vulnerability ⊑ T) defines a vulnerability on an asset, which refers to an infrastructure. Each individual of the Vulnerability concept can be exploited by an individual of the concept threat and can be mitigated by one or more individuals of the concept control. The severity scale of the Vulnerability concept is specified by the concept severity scale, which is defined as low, medium or high.
- A Threat is described as „Any circumstance of event with the potential to adversely impact an asset through unauthorized access, destruction, disclosure, modification of data, and/or denial of service“ (ENISA, 2016). An individual of the concept Threat (IT-Security: Threat ⊑ T) might exploit an individual of the concept Vulnerability. The concept Threat Type covers the name(s) of the Threat Type, e.g. Trojan Horse, Spyware. The concept Threat Status might either be active or inactive. The concept Threat Discovery gives information of the Threat Discovery Date. Each Threat has a Threat First Known Sample. Thus this concept covers the date of the threat first known sample. The concept Targeted Platforms covers the name(s) of the Targeted Platforms, e.g. Windows, Unix. To identify the relevance of a threat, the concept Top Targeted Countries covers the name(s) of the top targeted countries, e.g. Germany, Belgium. The concept Purpose Function e.g. cyber espionage covers the intention. The concept propagation way covers the name(s) of the propagation way, e.g. Social Engineering.
- The concept Control (IT-Security: control ⊑ T) defines how to mitigate vulnerability. Each control is specified by the concepts standard control, e.g. “Update Acrobate Reader” which is allocated to a control ID. The control ID indicates the ID of the aforementioned standard control “APSB13-7” and a committee. Further information of the control is given by the control type which might be corrective or preventive.

2.1.2 IT-Security: ABox Individuals

The following Figure 2 gives an example of the individuals for the TBox concepts.

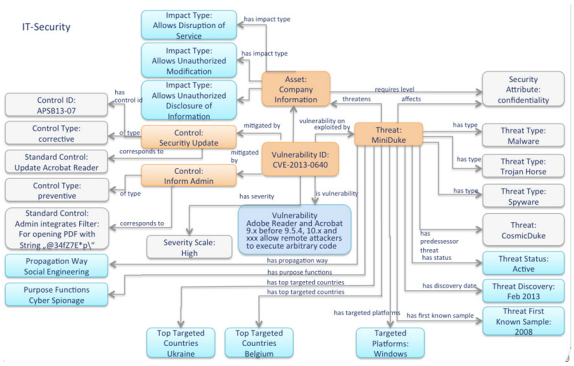

Figure 2: IT-Security Subontology ABox Individuals.

ABox individuals of the core TBox concepts Asset, Threat, Vulnerability and Control are depicted in orange. The blue TBox concepts are specific for critical infrastructures and the grey TBox concepts that are based on the Fenz ontology.

- Threat: The Threat MiniDuke (Raiu, Costin et al., 2013) threatens the Asset Company Information.
- Vulnerability: The Threat Miniduke exploits the Vulnerability ID: CVE-2013-0640 (CVE, 2013) which refers to a gap in the Adobe Acrobat Reader.
- Control: The Vulnerability is mitigated by the Control: Security Update and Inform Admin.
- Impact Type: The Asset Company Information has the Impact Type: Allow Disruption of Service, allows unauthorized modification and allows unauthorized disclosure of information, with potentially fatal consequences with regard to critical infrastructures.

2.2 Project Ontology

Subontology Project covers a cross sectoral analysis and classification of project information (for internal use in our research cluster) and results like project institution, competence, critical infrastructure and approach.

2.2.1 Project: TBox Concepts

The Subontology Project covers concepts of the research projects of the research programme ITS[KRITIS and information like partners, contacts and competences depicted in Figure 3. It links the information from the projects to approach/best practices. This information is relevant for initiatives that are part of the cooperative research process of ITS|KRITIS.

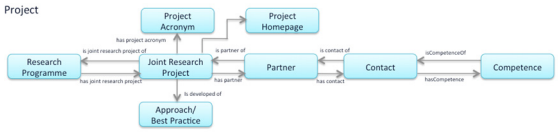

Figure 3: Project Subontology TBox Concepts.

2.3 CRITIS Ontology

2.3.1 CRITIS: TBox Concepts

The subontology CRITIS provides a framework which enables the presentation of the critical infrastructure. The subontology links the cross sectoral classification of the projects with critical infrastructure relevant aspects as Asset, Organization and Critical Infrastructure. Figure 4 depicts the concepts of a critical infrastructure.

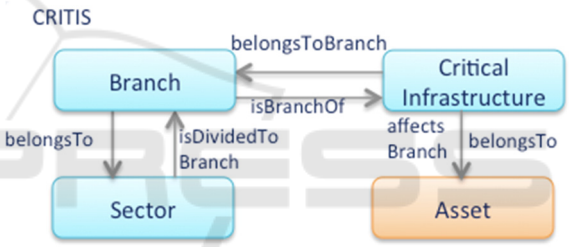

Figure 4: CRITIS Subontology TBox Concepts.

- According to (Innern, 2009) a critical infrastructure is defined as follows: “Critical Infrastructures are organizations and facilities with a great importance for the governmental community. Acting bottlenecks in supply that have a lasting effect, considerable disorganization of public security or other dramatic impacts are consequences on their breakdown or disturbance”. The concept critical infrastructure (CRITIS:critical infrastructure $\sqsubseteq$ T) is used to model an organization and facility which is assigned to as Critical Infrastructure. The relation from the Critical Infrastructure to its Assets is a core element of this ontology.
- Each Critical Infrastructure belongs to a specific Branch which is assigned to a Sector. For example the Branches electricity, mineral oil and gas are assigned to the Sector energy.

The IT-Security subontology is linked to the Critical Infrastructure Ontology (CRITIS) subontol-

ogy and consequently to the appropriate assets of a company.

2.3.2 CRITIS: ABox Individuals

Figure 5 provides examples of individuals for the TBoxes introduced in Sect 2.3.1. The Critical Infrastructure waterworks "SafeCity" is a short part of a "SafeCity" scenario. The Branch is waterworks which is Branch of the Critical Infrastructure "SafeCity". The waterworks "SafeCity" belongs to Asset company information. The Branch waterworks belongs to the Sector Energy.

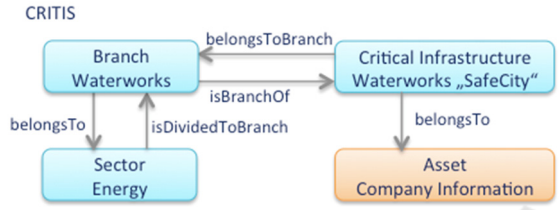

Figure 5: CRITIS Subontology ABox Individuals.

2.4 Compliance Ontology

The subontology Compliance covers norms and standards, regulations and applicable laws as well as measures.

2.4.1 Measures: TBox Concepts

In this paper, we introduce the subontology Measures as a part of the compliance ontology. The Measure subontology covers IT-Grundschutz Manual and Project concepts.
The main TBox concept of the ontology Measures is Measure, which is linked to the TBox concept Vulnerability via 'mitigated by measure'. Each Measure is linked to a Measure ID via 'has measure ID' and this in turn refers to a Comitee via 'refers to comitee'.

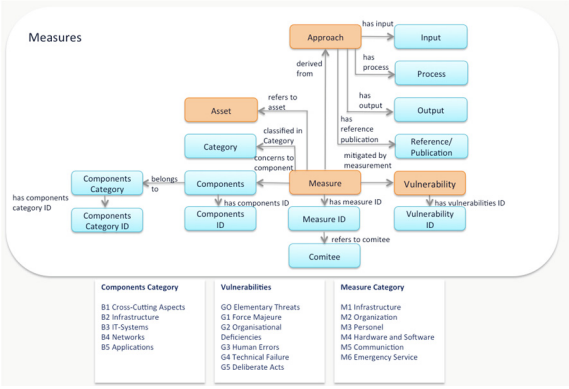

Figure 6: Measures Subontology TBox Concepts.

The following concepts are derived from the IT-Grundschutz Manual (BSI, 2013)

- Components Category (CRITIS:Measure:IT-Grundschutz Manual components categorie ⊑ T) is linked to a Components Category ID like B1 Cross-Cutting Aspects, B2 Infrastructure, B3 IT-Systems, B4 Networks and B5 Applications.
- Components (CRITIS:Measure:IT-Grundschutz Manual components ⊑ T) is linked to a Components ID belongs to a components category, e.g. "Handling Security Incidents" with the components ID "B 1.8" is linked to the components category via "belongs to" the components "Cross Cutting Aspects".
- Measure (CRITIS:Measure:IT-Grundschutz Manual measure ⊑ T) is linked to a Measure ID and concerns to a component e.g. "Detection and Recording of Cyberattacks" concerns to the component "Handling Security Incidents". Furthermore, a Measure is linked to a vulnerability of the IT-Security ontology (CRITIS:IT-Security vulnerability ⊑ T) via mitigated by vulnerability.

Additionally, our approach covers new measures that are derived from the approaches of the projects of the research programme ITS|KRITIS.

The Project subontology of (CRITIS:Project) provides a framework which represents the approaches from the project partners:

- The concept Approach (CRITIS:Project – Approach approach ⊑ T) introduces the approach from the project partner which is either classified in category as "New Approaches to assess the IT-Security" or "New Approaches to increase the IT-Security".
- The concept Approach is linked to the concepts input a defined process and output. Furthermore, links to references and publications are defined. The concept approach is linked to the concept Measures.

Another important concept in the subontology Measures is the link to the Asset of the Critical Infrastructure via 'refers to asset'. Thus, in case a Critical Infrastructure of the same or another Branch has the same Asset. It might be interesting to be informed of the Measure and consequently the appropriate Vulnerability.

2.4.2 Measures: ABox Individuals

The following Figure 7 provides an example of the individuals for the in 2.3.1 introduced concepts.

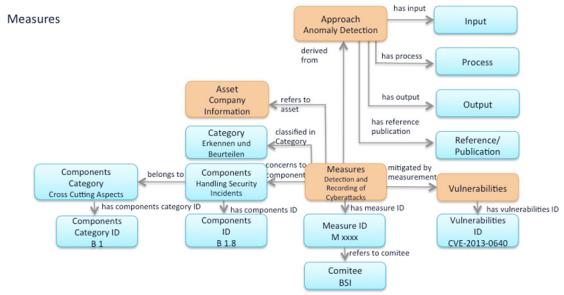

Figure 7: Measures Subontology ABox Individuals.

The Measure ‘Detecting and Recording of Cyberattacks’ with the Measure ID 123 refers to the comitee BSI. The Measure concerns to the component ‘Handling Security Incidents’ with the Component ID B 1.8, which belongs to the Components Category ‘Cross Cutting Aspects’ with the Components Category ID B 1. The Measure mitigates the vulnerability CVE-2013-0640.

The Approach Anomaly Detection from one of the ITS|KRITIS projects gives a further measure. The Measure is classified in category ‘Recognise and assess’ and the Asset in this case is the Company Information.

3 INTERPLAY OF CYBERSECURITY ONTOLOGIES

First, this section provides a short overview of the interplay of TBox concepts and, second, an example of the interplay on ABox level in section 3.2.

3.1 TBox Concepts

The following Figure 8 shows the interplay of the key concepts of the cybersecurity ontologies.

The cybersecurity ontology in this part of the overall ontology includes the subontologies Project, CRITIS, Measures (which is one part of the Compliance ontology) and IT-Security.

The Asset is the centre of the Cybersecurity ontology. The Asset ‘is Asset of’ a Critical Infrastructure, which refers to a branch belongs to a sector of the subontology CRITIS.

Furthermore the Asset affects all of the aforementioned subontologies: Project, CRITIS, Measures and IT-Security.

The most important interplay build the TBox concepts: The TBox concept Vulnerability is vulnerability on concept Asset. The Vulnerability on the other hand is exploited by a Threat and a Vulnerability is mitigated by a Measure.

As mentioned in the Chapter 2.4.2 the Measure might either be linked to a Measure ID of a Committee or to a specific Approach from our project partners.

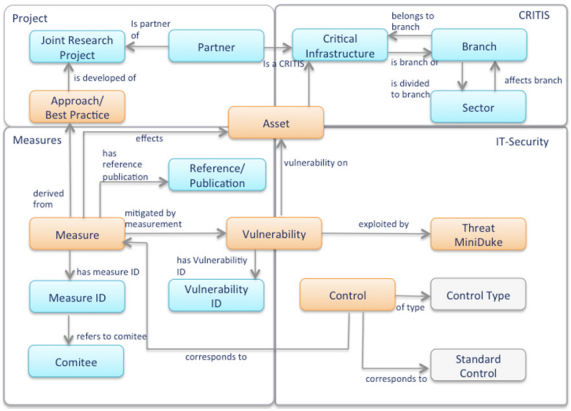

Figure 8: Interplay of TBox Concepts.

3.2 ABox Individuals

The Figure 9 shows the interplay of TBox concepts introduced in Chapter 3.1 with ABox individuals. The example is again a scenario relevant for Miniduke for the waterworks of the city “SafeCity”.

As mentioned in Chapter 3.1 the center of this ontology is the Asset, which in this example is the Company Information. The Asset is the asset of the Critical Infrastructure waterworks, which belongs to branch Energy Supply, which in turn is assigned to the Sector energy.

Another important concept and consequently individual is the Vulnerability, which is a vulnerability on the Asset. In this example the Vulnerability with

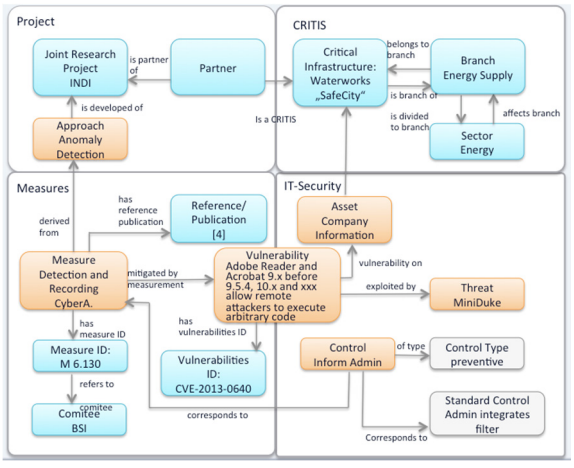

Figure 9: TBox Concepts and ABox Individuals.

the ID CVE-2013-0640 is used, which covers the Vulnerability "of the Adobe Reader and Acrobat 9.x before 9.5.4, 10.x before 10.1.6, and 11.x before 11.0.02 allow remote attackers to execute arbitrary code or cause a denial of service" (CVE, 2013). This Vulnerability is exploited by the Threat MiniDuke.

The Vulnerability might now be mitigated by the Measure detection and recording Cyber Attacks. The Measure has the Measure ID M. 6. 130 and comes from the Comitee BSI.

What should be done now? The Control 'Inform Admin' of the type control type preventive should be executed. This control corresponds to the standard control 'admin integrates filter'.

Thus, the waterworks is aware of the aforementioned vulnerability in the Acrobat Reader.

4 CONCLUSION AND FUTURE WORK

We have introduced the subontologies that are used for the Cybersecurity ontology. Additionally, we have introduced TBox concepts and ABox concepts for the subontologies. Furthermore, we have introduced the interplay of the Cybersecurity subontologies on both TBox level and ABox level.

In future we will work on ABox individuals with the results from the research projects of ITS|KRITIS.

For this step we will define an interactive process to interact with the research projects of ITS|KRITIS. We will define a process to validate and release this ontology with roles.

Furthermore, we investigate in intelligent Security Level forms which might be based on (Bergner, 2015b) and (Bartelt et al., 2016). The ontology will be integrated in the common project platform www.itskritis.de.

ACKNOWLEDGEMENTS

We acknowledge the funding of VeSiKi by the BMBF (FKZ:16KISO213) and the VeSiKi team fruitful discussions.

REFERENCES

Bartelt, C., Bergner, S., Bergner, K., Rausch, A., 2016. Methodology for an Ontology-Driven Product Configuration Process. *Ilmenau*.

Bergner, S., 2015a. VeSiKi-Project: Ontologies for IT-Security in Critical Infrastructures. P*resentation at the IC3K, Lissabon.*

Bergner, S., 2015b. Towards Automated Integrity Constraints Modelling and Validation: A Survey and Approach. *Presented at the KEOD, Lissabon.*

ISO, 2013. ISO 27001.

CVE, 2013. Common Vulnerabilities and Exposures for the Vulnerability: CVE-2013-0640.

ENISA, 2016. ENISA European Union Agency for Network and Information Security.

Fenz, S., Ekelhart, A., 2009. Formalizing information security knowledge, in: Proceedings of the 4th International Symposium on Information. *Presented at the ACM, ACM, Sydney, Australia, pp. 183–194.*

Innern, B. des, 2009. Nationale Strategie zum Schutz Kritischer Infrastrukturen (KRITIS-Strategie) 20.

BSI, 2013. IT-Grundschutz Catalogues.

Kaspersky, 2016. Kaspersky Security List.

NIST, 2016. National Vulnerability Database.

Raiu, Costin, Soumenkov, I., Baumgartner, K., Kamluk, V., 2013. The MiniDuke Mystery: PDF 0-day Government Spy Assembler 0x29A Micro Backdoor.

Stonebumer, Gary, Goguen, Alice, Feringa, Alexis, 2002. NIST information security risk management guide, *NIST Special Publication 800-30. NIST National Institute of Standards and Technology.*

Tsoumas, B., Grizalis, D., 2006. Towards an Ontology-based Security Management. *IEEE, Austria, Vienna.* doi:10.1109/AINA.2006.329.