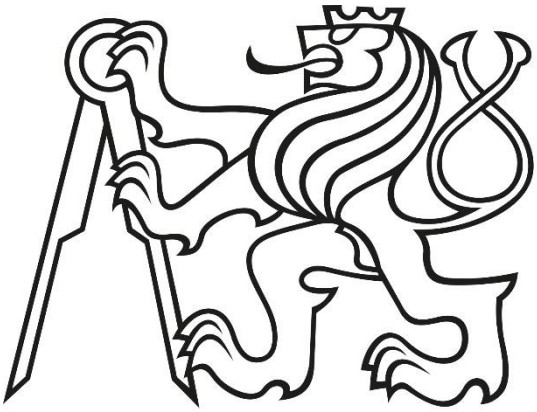
CZECH TECHNICAL UNIVERSTITY IN PRAGUE
FACULTY OF ELECTRICAL ENGINEERING
DEPARTMENT OF TELECOMMUNICATIAN ENGINEERING

Bachelor's thesis

Cybersecurity in the Czech Republic



Study programme: Communication, Multimedia and Electronics

Specialisation: Network and Information Technology

Bachelor Project Supervisor: Ing. Pavel Bezpalec, Ph.D.

May 2016 **Filip Řežábek**

Poděkování

Děkuji Ing. Pavlu Bezpalcovi Ph.D. za odborné konzultace, připomínky a cenné rady, které mi předal při vypracovávání bakalářské práce. Děkuji také své rodině, která mi poskytla potřebnou podporu po celou dobu mého studia. Děkuji také panu Michalovi Zedníčkovi ze společnosti Alef Nula a.s., za rady a konzultace, které napomohly k dosažení cíle.

Čestné prohlášení

Prohlašuji, že jsem zadanou bakalářskou práci zpracoval sám s přispěním vedoucího práce a konzultanta a používal jsem pouze literaturu v práci uvedenou. Dále prohlašuji, že nemám námitek proti půjčování nebo zveřejňování mé bakalářské práce nebo její části se souhlasem katedry.

Datum:

……..……

podpis bakalanta

České vysoké učení technické v Praze
Fakulta elektrotechnická

katedra telekomunikační techniky

ZADÁNÍ BAKALÁŘSKÉ PRÁCE

Student: **Filip Řežábek**

Studijní program: Komunikace, multimédia a elektronika
Obor: Síťové a informační technologie

Název tématu: **Kybernetická bezpečnost v ČR**

Pokyny pro vypracování:

Proveďte řešerši legislativních dokumentů vztahujících se k problematice zákona o kybernetické bezpečnosti v podmínkách ČR. Proveďte průzkum trhu a identifikujte národní či mezinárodní certifikační programy, které jsou nutné pro výkon rolí Architekta, Manažera a Auditora kybernetické bezpečnosti dle zákona. Na základě těchto poznatků navrhněte znalostní a kompetenční profily, které musí uchazeč o tyto role získat, aby byl připraven na výkon povolání v této roli. Zároveň zmapujte nabídku školení soukromých a státních institucí, které slouží jako příprava na výše zmiňovaný typ certifikace.

Seznam odborné literatury:

[1] *Zákon č. 181/2014 Sb. o kybernetické bezpečnosti.* Dostupné na https://www.zakonyprolidi.cz/cs/2014-181 [on-line].
[2] *Vyhláška č. 316/2014 Sb. o bezpečnostních opatřeních, kybernetických bezpečnostních incidentech, reaktivních opatřeních a o stanovení náležitostí podání v oblasti kybernetické bezpečnosti.* Dostupné na https://www.zakonyprolidi.cz/cs/2014-316 [on-line].
[3] *Vyhláška č. 317/2014 Sb. o významných informačních systémech a jejich určujících kritériích*. Dostupné na https://www.zakonyprolidi.cz/cs/2014-317 [on-line].

Vedoucí: Ing. Pavel Bezpalec, Ph.D.

Platnost zadání: do konce letního semestru 2016/2017

prof. Ing. Boris Šimák, CSc.
vedoucí katedry

prof. Ing. Pavel Ripka, CSc.
děkan

V Praze dne 21. 12. 2015

Anotace

Tato bakalářská práce se zabývá dopadem nově vzniklého zákona 181/2014 Zákon o kybernetické bezpečnosti na území České republiky prostřednictvím vytvoření kompetencí rolím vyplývající z něj a zmapováním nabízeného profesního rozvoje. Pro definování kompetencí jsou využity vyhlášky 316/2014 Sb. a 317/2014 Sb., normy rodiny ISO/IEC 27000, ISO/IEC 19011, ITIL v3, dále jsou zkoumány požadavky pracovního trhu a mezinárodní certifikační autority. Dále byly promítnuty zkušenosti z práce na projektu Analýza rizik v rámci rozsáhlé telekomunikační společnosti. Ta hraje klíčovou roli pro definici efektivních bezpečnostních opatření, a to jak technických tak organizačních. Je kladen důraz na specifické zodpovědnosti jednotlivých rolí za využití topologie, se kterou daná role pracuje.

Klíčová slova

Incident, analýza rizik, zodpovědnost, opatření, hrozba, zranitelnost, bezpečností politika, proces, ISMS, kompetence, role, zákon

Summary:

This bachelor thesis deals with impact of incoming law 181/2014 Cyber security law in the Czech Republic. Impact is analysed by creation of a role model and specifying role's competencies mentioned in the law by mapping professional development. Competencies are defined based on regulations 316/2014 Coll. and 317/2014 Coll., family of ISO/IEC 27000, ISO/IEC 19011, ITIL v3, examination of job market and international certification authorities. Further is involved professional experience from Risk Analysis project in Telecommunication Company. Risk analysis plays a key role for definition of effective security measures, covering technical as well as organizational measures. There is strong emphasis on specific responsibilities of each role by usage of a topology, which is given role working with.

Index Terms:

Incident, Risk analysis, responsibility, measures, threat, vulnerability, security policy, process, ISMS, competence, role, law

Table of Contents

1 Introduction – The motivation for Cyber security 1
2 Historical development of Cyber security in the Czech Republic 3
2.1 Economical and technical part of the issue 3
2.2 Progression of Cyber security law 4
2.3 Specific principles suggested for the act of legislation 5
3 Cyber security law and regulations 8
3.1 Cyber security law 181/2014 Coll. 8
3.1.1 Paragraph 5 10
3.1.2 Paragraph 8 14
3.2 Regulation 315/2014 Coll. 15
3.3 Regulation 316/2014 Coll. 16
3.4 Regulation 317/2014 Coll. 17
4 Cyber security roles 19
4.1 CERT/CSIRT 19
4.2 Manager 22
4.3 Architect 26
4.4 Auditor 30
4.5 Asset Administrator 33
4.6 Incident Manager 35
5 Professional Development 37
5.1 International Certification Authorities 37
5.2 Public schools 39
6 ISO 27k Family 40
6.1 Information security risk management – ISO 27005 40
6.2 Risk analysis – Telecommunication operator 41
7 Conclusion 43
8 References 45
9 Table of Figures 47
10 Vocabulary & List of Shortcuts 48

1 Introduction – The motivation for Cyber security

Firstly, motivation of this thesis has to be mentioned, why to focus on Cyber security issue. As the Information and Communication Technology (ICT) started to involve our lives more and more, started to be connected with general improvement of society and development of services, many people do not realize the threats coming with it. Improvement goes in hand with dependency on ICT, since it is connecting families, companies, states and especially its critical infrastructure.

An important milestone for Cyber security development as it is known today was the first global attack in 1988, which was done by 23 years old student of Cornelly University. This attack was named after him and it is the Morris Worm. As a result of this attack, people started to realize the threat coming with their high–tech computers. Even at that time there was not the Internet like it is known today, but the worm was moved through floppy drive and despite of that infected thousands of computers. As a reaction to this threat was set up first Computer Emergency Response Team (CERT) at Carnegie Mellon University in the United States.

Next step was computers implementation to government services and digitalization of important data. The American National Security Agency (NSA) started to realize their value and possible danger coming with it. As a result started American government, especially NSA cooperate with CERT at Carnegie Mellon University, because of their previous experience with Morris Worm and other threats in meanwhile. After improving relations and increasing prestige of Carnegie Mellon was developed new area and it is called ICT Security.

Current topics of ICT world are Internet of Things, Industry 4.0, Cloud computing and many more, which have in common connection to the Internet. Unfortunately the usage of modern technologies is increasing the number of risks and violence in Cyberspace. As a result of these threats came the Information Technology Security or Cyber security. Cyber security has a main aim to protect the Cyberspace by protecting the information systems (IS) and critical infrastructure. It is necessary to say that Cyber security started to be mentioned since beginning of 21st century, but as are all these “Smart” gadgets surrounding us, the need for Security is higher than ever. To give an example, try to think about a power plant, which is attacked. This problem is connecting the digital world with physical, real world, which can affect all of us. In general attacks can have huge economic impact in both private and public sector. By attacking the critical infrastructure may be questioned even the safety or independence of state. One of the challenges is to keep up with the hackers, since their attacks are more sophisticated, complex and their area of focus is moving from individual interest to Cyber spying or terrorism. This tendency can be seen in current wars in the Middle East.

What is understood by the “critical infrastructure”? Among critical infrastructure belongs power system, logistic channels, medical facilities, industry facilities, banks, and IS of public administration and many more… Unfortunately for Cyber security experts, Cyberspace does not have any borders, so it is necessary to handle it on international level. The Czech Republic is a member of European Union (EU) and North Atlantic Treaty Organization (NATO) and has to fulfil the commitments. As a result Czech has to come up with a legal regulation regards to this issue. Each country has to introduce a strategy, naming national Authority responsible for safety of networks or infrastructures and establish a response CERT on National and Government level.

It is necessary to say, that Cyberspace is and will be under close watch of supervisory authorities. The main authority in Czech is the National Security Authority (NSA), under which

was established in 2011 the National Cyber security Centre (NCSC), which includes government CERT. Since it is absolutely essential to centralize the information about attacks and create ad hoc solutions, has to exist an authority, which is able of that, which is and has to be the state. State has this responsibility, to protect and help people identify and protect their informational self–determination. Only the state has the legislative possibilities how to control and demand the implementation of security solutions.

Unfortunately in the public administration does not exist uniform security standard that would minimize the damage after an attack, neither prevent nor warn before the attack occurs. On the other hand in private sector are mostly applied ISO/IEC standards 20000 or 27000. Even though the state does not dispose with any competence to divert a Cyber–attack, security measures can give additional time to handle the incident.

Before it is proceeded, it has to be mentioned that the Czech Republic is one of few countries or maybe even only one within Europe which has own Cyber security law. The European Union is coming with its Network Incident Security (NIS) directive which should have been published at the end of 2014, which did not happen, so it was delayed for 18 months and in the end it might be published at the turn of 2016/2017. This directive will mean novelization of current Cyber security law and regulations, which has been already in preparation.

2 Historical development of Cyber security in the Czech Republic

First concepts or drafts were introduced in 2001 in strategy of the Ministry of the Interior against the organized crime. At that time were firstly presented the problems with cybercrimes. Many organs like police, intelligence agencies supposed to create teams focused on upcoming problems. These organs should prepared threat scenarios, alert systems, and educational system for employees and last but not least name CERT to supervise this issue. These strategies were developed through years 2005, 2007, 2010, 2011 and 2012 and next wave is expected in the beginning of 2016. As the Cyber security became more realistic threat the improvement has to go in hand to keep with assailants. Year by year new items were added to concepts, like protection of critical infrastructure, real–time monitoring of threats, auditing of current solutions, international cooperation, investments to education and increase of public knowledge, gathering, analysing and evaluation of existing accidents and the most important creation of legislative support. New teams called Computer Security Incident Response Team (CSIRT) were established and their cause is to take some responsibilities from NSA, since they are more experienced and are cooperating on international level. In general it is necessary to work on international level with involving of private institutions and experts from professional public.

In conclusion the main target is to create a complex security measure, detection of cyberattack events, its reporting and counteractions to threats. In charge of it would be two CERTs on national and government grade.

2.1 Economical and technical part of the issue

Project like Cyber security will require funding all the time, since it is never ending project, since the necessity of improvement, research and protection is daily routine of security experts. However there should not be so much additional costs to private sector, because the subjects where is protection required have already implemented security mechanism regards to the international standards ISO/IEC 27000, ITIL or any other recommendation. If a company received certificate that their system fulfils the audit requirements, they do not have to take in account additional costs.

There are different scenarios how a state can act and each has own pros and cons [4]:

1. Zero variant

Unfortunately zero means continuing in status, where is no specific law treatment nor centralizing institution. As a result only private sector or voluntary organizations would look after own infrastructure trying to know what is happening on their perimeter. This system is sensitive to passive attitude of each involved institutions. In general it would bring just huge security risk and almost zero change of facing the attacks on international scope. It might look, that it is money saving, since the state does not have to invest in setting up centres or teams, however each institution would have to invest to create own problem solution and implementation. The biggest disadvantage is hoping that your "neighbour" would do the same, if he does not, your network is in danger. This would result in infective and money demanding solution. Someone would say that the state resigned on protection of basic rights. In addition it would bring international problems, since the due diligence rule would not be met.

2. Protection of Information system with sensitive data

In this case have the protection would limited scope covering only systems with sensitive data. An investment would not be so high, since many protection mechanism are already implemented. However this range is covering only one of many critical infrastructures. The current trend is moving more information to virtual world and it is closely bounded with economic or political activities. From this it may be seen that protection of specific field would not solve a complex problem.

3. Public Information system protection

This can be understood as opposite of "Zero variant", since state would protect only own infrastructure, which would be easier to implement and control. However most of communication networks are owned by private sector which would be unprotected. This scenario would work only in totalitarian form of state, where everything is owned by state and would not bring any improvement to basic security questions.

4. General activity and a cooperation with private sector

Basically it can be understood as a combination of public and private sector, where private sector is independent, can implement own solution and this security solution is generating profit to companies. With secured infrastructure is company offering confidentiality, integrity and availability (CIA) of data and people are willing to pay for their services. Each infrastructure designer knows his system. In contrast with "Zero variant" this solution is more effective and would be the best for the Czech Republic.

5. General activity and direct regulation

Direct regulation means that NSA would have legislative competencies to interact and interfere with security solutions in each IS. All the responsibility would be on NSA, since all the systems would be under their control. This would bring huge technical and organization problems as well as direct costs. From this aspect it looks almost unrealistic.

However handling Cyber security issue in Czech can bring many benefits.

- Competitiveness with other companies in Central Europe
- Trustworthy which can result in external investments
- Suppliers support of safety ICT solutions
- Protection of critical infrastructure which can bring confidence in state apparatus

It is worthy to mention that every year is budget for NSA increased and new work positions are opened. Generally speaking security experts are demanded in private as well as public sector.

2.2 Progression of Cyber security law

The proposed solution of Cyber security law:

The best solution would be to create a law in the combination with private subjects, since they are experienced in maintenance and knowledge of their own infrastructure. The other two possibilities – direct regulation or particular legislative limitations are not possible, since Cyber security is a complex problem and its regulations are in conflict with constitutional laws.

In the created law, which is partially inspired by current laws is necessary to specify jurisdiction of NSA, its control mechanism and sanctions. Moreover, it has to explain own

notions, regards to Cyber security – as an example can be taken “Status of Cybernetic danger”. Next step in development is to specify responsibilities of NSA and National and Government CERT teams.

Efficiency reporting of suggested law was done in three ways:

1. Observation of technical development and review of security precaution implementation

NSA is observing through National and Government CERT, cooperates with international partners and solves current problems or improves the system. It goes in hand with update of suggested legislative apparatus.

2. Scoring of legal adjustments and structure parameters

Periodical checks respecting new standards and best practices implementation.

3. Scoring effectiveness of law justice

Scoring was done in cooperation with private sector and academically researchers. If it is found a shortage of legislative competence, the organizations have to adapt quickly, especially in the area of ICT will this happen often.

Before the Cyber security law was officially released, plenty of consultation were held among academia, private and public sector, professional public, NSA, international partners, NCSC and other partners. All the meetings, workshops were really helpful and gave many new suggestions and ideas how to develop the concept. Since it is a really complex problem, the best approach to create apparatus was with joint forces.

In addition, it is important to mention which international partners were involved. First contact was with foreign CERTs, NATO Cyber Defence management (memorandum was signed), EU countries, CIA, FIRST (Forum of Incident Response and Security Teams), ENISA (European Network and Information Security Agency), AFCEA (Armed Forces Communications and Electronics Association), ITU (International Telecommunication Union) and ISACA (Information systems Audit and Control Association). The cooperation was mostly based on participating on conferences held by mentioned organizations, visits of their centres for inspiration, sharing knowledge databases and many more.

However it is not only about the legislative but as well about the technical possibilities of involved subjects. It was chosen to send a detailed survey to each subject of critical ICT infrastructure. This approach is the fastest and cheapest for NSA and companies. As a result was found out that around 80% of subjects are using standards ISO/IEC 27000 which is Cyber security law based on.

2.3 Specific principles suggested for the act of legislation

It cannot be omitted, that the created law is based on several key principles. The difference between normal laws and Cyber security law is in the purpose of it. The aim is not to penalize the criminals, attackers or hackers, but to give the best recommendations, measures and scenarios which result in protection of Critical infrastructure and ensure its smooth run even under attack. It is possible to divide the principles into several categories [4]:

1 Technological neutrality

In this category the state will not censor the communication data and will not control the suppliers. Basically saying, the owner of ICT infrastructure has to fulfil given requirements, but the control authority cannot choose which supplier and product will be chosen for protection.

2 Protection of informational self–determination

Secondly, it is said that each person should be allowed to communicate with the world. Firstly was the self–determination understood passively – protection of privacy. However the self–determination was enriched by adding the active part of understanding, which means that each person should be able to actively receive, utilize and communicate in Cyber space. The tools for protection should not be used for identification of people and stealing their privacy.

3 Protection of non–distributive rights

Thirdly, non–distributive rights are about protection of key functionality of state, internal security and protection against noxious consequences. It has been decided to cover these matters since more information systems are integrated into state infrastructure. The attack may result in crippling of energy supply and other essential commodities for mankind.

4 Minimization of state coercion

Next part means, that the private sector has duty to fulfil the importance of Cyber security law only in case, it belongs to Critical infrastructure. Despite that many other private companies can collaborate freely, without coercion of the state, which results in better cooperation and experience sharing. The government CERT should be opened to collaboration. The status of Cybernetic danger can be announced only by the Prime minister, after that it has to be confirmed by the government of the Czech Republic. It all has to be done under recommendation from the NSA director.

5 Autonomy of regulated subjects

Each institution that belongs to Critical infrastructure is different and as a result there is very heterogeneous group of subjects. The approach that was chosen counts with it and does not give specific technical nor organizational methods how to protect own network. There is given list of what should each subject be able to handle, but the procedure and responsibility to achieve given task is on each one of them.

6 Due diligence to international partners

As a member of international network, it is our duty to protect Czech infrastructure in relation to our neighbours. The infrastructure should be protected. Every attack with source in Czech must be detected shortly after it starts or even better the attack should not even begin. This results in creation of secured network for our nation and our partners.

From these principles it can be seen, that the Cyber security law is very different from other laws and it can be said that it is closer to recommendation with respect to all involved institutions than so far known laws. However there has to be control mechanism how to regularly check and improve current vulnerabilities. In each institution will be a team of security experts, who will communicate with national or government CERT and report attacks to them. The created database of attacks will help to minimize vulnerabilities in other systems. The CERTs will also be representatives who will cooperate with international CERT teams. The role of NSA is giving retaliatory measures against current threats. The government CERT will

be focused on control of Critical or Significant infrastructure for smooth run of the state. In addition NSA has the right of penalizing. On the other hand national CERT collaborates mostly with private sector and its CERTs.

Besides, the role of controlling is given to Ministry of the Interior, since it is the most experienced organization and has resources for that. Their knowledge was seen at the first steps of Cyber security law.

All the factors which stood behind creation of the Cyber security law in the Czech Republic were fully considered. Since it is a new law, there is high possibility that amendment will have to be written. Moreover, it is important to mention that ICT is fast changing area and the standards, recommendations or laws have to go in hand with it, otherwise it will slow down the improvement and attackers will be many steps ahead. For example in last years was common DDoS (Distributed Denial of Service) attack, however the attackers are using these years Social engineering. In conclusion was chosen unique approach how to write the law, since many organization from both private and public sector were involved, asked and collaborated on common target – creation of a new law, which moves the Czech Republic forward.

As a result the law is covering all the mentioned principles, is defining the tasks to owners of Critical and Significant infrastructure, specifies the role of National and Government CERT and is opened for future development. The need of that law is noticeable from the will of organs to create it. However the law is not the only thing which has to be done. There is also a problem with human resources, since there is worldwide lack of cyber experts. For minimizing this lack has to be opened new majors at high schools and universities after their competences are defied. Moreover, many people do not realize the threat which can wait in Cyberspace and is worthy to raise public awareness, especially for young generation which is in touch with ICT since they are born and are most vulnerable. Next problem is to motivate companies to invest enormous money to their equipment, since it is not generating any profit, however it is important to work with data CIA. If those three basic rules are not fulfilled, the trust given to institution may be lost, which might even result in bankrupt.

3 Cyber security law and regulations

It was discussed which steps led to creation of the law 181/2014, Cyber security law and in this chapter will be closely introduced the law itself, with its structure and important parts. The parts important for the scope of this thesis are paragraph 5 with its organisational and technical measures and paragraph 8 with Incident reporting system. Next part is covering regulations, which came with the law. Concretely it is regulation 315/2015 Criteria for Critical Information Infrastructure, 316/2014 Cyber security regulation and 317/2015 about Significant Information Systems and defining criteria.

These legislative documents are combining recommendation with practical tasks how to do ensure infrastructure security. However fulfil legislation does not mean only to buy equipment, but it is also its maintenance, optimization and comprehend in processes.

3.1 Cyber security law 181/2014 Coll.

The Cyber security law is a result of Strategy 2015, which set these goals:

1. Creation of a legislative tool – Cyber security law
2. Organization structure – National and Government CERT
3. Education and increase of public awareness

The first two goals are fulfilled, however in the case of third it is difficult to say. There is no regular major at many universities and there is no major for high schools or elementary schools. This might be changed in next years, but because of slow and indecisive behaviour of state organs it takes time. In case of high schools will be introduced Cyber security major in pilot testing in school year 2017/2018 at Secondary technical school, Smíchov and partner school in Brno. This activity is due to Sector agreement, where are other activities creation of study packages, which will be implemented to education system on elementary schools and other high schools. Many organization signed this agreement, which is a result of previous funding.

In the following strategy 2016 – 2020 is taken into account development of stable education background by setting up a training centre for testing, sharing gained experience and know–how with professionals.

The Cyber security law was published on 23 June 2014 and is effective from 1 January 2015. Generally saying, the law has 11 pages, 6 Chapters and 38 paragraphs. Here is short overview of each paragraph.

For the scope of this thesis are important definitions of:

- Critical Information Infrastructure (CII) – part of Critical Infrastructure.
- Information System for CII – part of Critical Infrastructure with aim to process information.
- Communication System for CII – part of Critical Infrastructure with aim to designate purpose of communication.
- Significant Information System (SIS) – in case of failure can effect public administration and bring confusion.
- Significant Network – provides international connection or directly connects Critical Information Infrastructure.

38 paragraphs are as follows:

- § 1 – Subject Matter – gives brief information about scope of the law.
- § 2 – Definitions – vocabulary list of key words related to cyber security, for example understanding of Critical or Significant infrastructure.
- § 3 – Compulsory subjects – defines which person or institutions belong to the cyber security law and have to satisfy its needs.
- § 4 – Security measures – definition of security measures and who is responsible for them.
- § 5 – **Demarcation of security measures** – defines the boundaries by distribution into organizational and technical measures.
- § 6 – Content of the implementing regulations – gives brief overview of regulations.
- § 7 – Definition of cyber security events and cyber security incidents – difference understanding between an event and an incident.
- § 8 – **Cyber security incident reporting** – informs who has the duty to report and to whom should the reports go.
- § 9 – Cyber security incidents records – names the responsible record holder, defines the possible cooperation among CERTs on national or international level.
- § 10 – Obligation of confidentiality – specifies which employees should be confidential and under which circumstances can they break their duty.
- § 11 – Action – definition of countermeasures and its categorization – warning, reactive or protective measures.
- § 12 – Warning – who recalls warning and has the right to it; Cyber security danger.
- § 13 – Reactive measure – regards to definition of subject duties by informing about result of counteraction.
- § 14 – Protective countermeasure – the NSA responsibility to avoid same incident in the future by information gathering of incidents.
- § 15 – Procedure for issuing a general measure – duty of informing about the incidents.
- § 16 – Contact information – specifies the necessary information, which should be provided to NSA, includes the reason for that. Next part is about taking into account the privacy of these information.
- § 17 – National CERT – responsibilities of team, its naming and defining its rights.
- § 18 – Operator of National CERT – specifies who can be named to the position of national CERT.
- § 19 – Public agreement – defines the requisites of contract between the NSA and National CERT operator.
- § 20 – Government CERT – by obligation has to be part of NSA, definition of its responsibilities and collaboration with National CERT.
- § 21 – Characteristics of Cybernetic danger state – definition of this status, responsible people for incident handling, its duration and cancellation.
- § 22 – State administration – the duty to name NSA and specifies their responsibilities and duties.
- § 23 – Control – NSA controls subjects if they fulfil their duties, for example improvement of their infrastructure after an incident by audit.
- § 24 – Corrective measures – in case NSA finds gaps it gives recommendation, how to minimize these insufficiencies.
- § 25 – Administrative offenses of legal entities and entrepreneurs – defining under which conditions the subjects commit an offense.
- § 26 – Offence – informs about possible offence penalization.

- § 27 – Consideration of an administrative offense – defines under which conditions can be the subjects omitted from penalties.
- § 28 – Empowering provision – the role of regulation and responsible ministry for their creation.
- § 29 – The period for fulfilment of obligations – defines after how many days owners of information infrastructure have to fulfil their duties regards to law and regulations.
- § 30 – Satisfying the obligations of administrators for information and communications systems in Critical information infrastructure – set dates after which should be improved their infrastructure to accomplish given tasks.
- § 31 – Satisfying the obligations for significant infrastructure administrators – names dates after which should be improved their infrastructure to accomplish given tasks.
- § 32 – Administer activity – gives information under which conditions works National CERT.
- § 33 – Common regulation – describes which institutions have to take this law into account – CII and SIS.

Paragraphs 34 – 37 are about changes in current laws and § 38 is the data when becomes law effective [4].

As is shown, the law is not so long and from its reading it is recognizable that it is written quite openly and does not specify almost anything. This is done by purpose, since ICT is fast developing and all the time changing environment and updates of law to its current needs is difficult or almost impossible task. As a result were written 3 important regulations – 315/2014, 316/2014 and 317/2014. They are closely described in next chapters. Regulations have an advantage in faster publication of amendments.

For the scope of this thesis are necessary these paragraphs:

- § 5 – Demarcation of security measures – defines the boundaries of IS by distribution into organizational and technical measures.
- § 8 – Cyber security incident reporting – informs who has the duty to report and to whom should the incident reports go. In addition, it defines the system of CERT and difference between National and Government CERT.

3.1.1 Paragraph 5

As it is mentioned above, the security measures distribute into organizational and technical. Information from Cyber security regulation are included within these specifications, nevertheless they are closely described in each paragraph of 316/2014 regulation [2].

The organizational measures are [4]**:**

a. Information Security Management System(ISMS):

By ISMS is meant management of assets and its aim is to eliminate their loss or damage by using risk assets, which should be protected by countermeasures and their periodical controls. In addition it gives approach to analyse and solve risks within information or communication systems. It covers needs of definition, monitoring, controls and systematic improvement of information security. It is necessary to define different rules based on subject's category (Information or Communication System of Critical infrastructure or Significant Information Infrastructure). Based on the rules, are introduced administrators duties. However requirements are taken from ISO/IEC 27001 "Plan–Do–Check–Act" (PDCA) cycle. Where CII has to fulfil

whole cycle and SIS only part of it. In case of CII are required periodical audits and effectiveness measurement of ISMS (at least 1 per year). Based on results should be the system updated. On the other hand SIS has to be checked only once per 3 years, however has to create complex security policy and processes related to that, too.

b. Risk Management:

Risk can be understood as probability, that a threat will use vulnerability of the system by negative influence of assets. In general, each subject belonging to Critical or Significant Infrastructure has to create own methodology for risk analysis, identify the risks and their possible impact and based on that create a report and apply the given recommendations to minimize the possible impact. CII risk analysis covers all assets, on the other hand SIS only describes primary assets. Risk analysis should include Statement of Applicability (SoA). One of the inputs for risk analysis is database of known vulnerabilities and incidents.

c. Security Policy:

Is a set of rules defining how should be dealt with sensitive information. For CII it has 21 areas and for SIS it is only 14. In case of CII it is basically covering all organizational and technical measures including "Bring Your Own Device" (BYOD) or "Choose Your Own Device" policy, archiving policy, cryptography protection policy, licencing or administration of technical vulnerabilities.

d. Organizational Security:

The administrators of Information or Communication System of Critical infrastructure should name following Cyber security positions:

- Manager – experience in running ISMS.
- Architect – creates and implements security countermeasures.
- Auditor – audits regularly and should be independent.
- Asset administrator – administrates given asset and works on its enhancement.
- Steering committee – team works on development of system improvement.

The roles are closely analysed in the following part of this thesis with suggestion of experience, education and their basic competences. It is shown by graphically illustrated approach to the "topology" they are in charge of. For all roles is required minimum three years of previous experience in security.

e. Addressing Security within Supplier Agreements:

Since owners of assets cannot improve infrastructure without touch from outside, it is necessary to sign agreements with trustworthy suppliers and periodically check their confidentiality.

f. Asset Management:

Asset is something valuable for public administration, organization or single person. It is differentiated between primary and subsidiary assets. Primary asset can be for example know–how and it is non–expandable for asset owner. Support asset are labours, suppliers and technical or software equipment. It plays key role to evaluate the impact of each asset loss. CII has to identify and keep records of subsidiary assets, specify their administrator and map and evaluate relation between primary and subsidiary assets.

g. Human Resource Security:

Each labour brings a risk, which can be limited by employee role specification and evaluation of their possible impact to the infrastructure, in case they are not well cared, educated or paid. Manager should not take this knowledge lightly and must prepare personal development plan and close evaluation of employees' skills, knowledge and experience.

h. Operation and Communication Management of CII and SIS:

Running and minimizing possible impact of security incident by implementing a set of rules, which are defining duties, responsibilities and procedures for that. It includes workflow, backup policy, development policy (distinguish between testing and work environment) and ensure CIA of transferred data. For CII and SIS are used tools specified in Technical measures f–h.

i. Access Control in CII and SIS:

Both SIS and CII have duty to control Access management and protect data authorization. However CII has to define rules for access management like unique ID, privileges, passwords and their update. Furthermore, rules should cover usage of Mobile devices owned by employer or employee. Usage of such devices brings potentially risk to the infrastructure and should not be underestimated.

j. System Acquisition, Development and Maintenance of CII and SIS:

It is mandatory to systematically improve administrated infrastructure, since threats are evolving as well. However the improvement can bring unwanted security exploits. As a result possible improvement has to be mentioned in Risk analysis. During development should be differentiation between testing and hard data and security testing has to be done before implementation. If are found lacks process should be returned back to beginning of development cycle.

k. Security Event and Security Incident Management:

Covers set of rules how to handle events and incidents. Every possible notification from security roles has to be analysed and evaluated. This goes in hand with incident analysis and its countermeasures and future improvement or system patching. In general it is a list of processes how to handle incidents with proper countermeasures.

l. Business Continuity Management (BCM):

BCM describes a process based on analysis of critical parts and processes within organization how to handle unwanted and unexpected events. It covers administrator duties and one of the most important is to develop continuity plan. By administrator is meant asset owner/administrator or other security roles. In the continuity plan has to be mentioned minimal possible service availability, recovery time to minimal functionality and normal availability.

m. Control and Audit of CII and SIS:

The control or audit of infrastructure is inseparable part of administrator work. Audits have to be done periodically by qualified person. Evaluation process covers fulfilling of legislative standards, security policy, BCM and Risk handling processes. The qualification of auditor will be introduced in next chapters.

The technical measures are [4]:

a. Physical Security

By physical security is meant protection of technical assets like servers, surveillance centres or any tangible or intangible goods as well as data. It can be done by mechanical protection (locks, chains …), detectors, fire protection, CCTV, UPS and so on. Buildings, rooms and possible entrance should not be omitted and has to be secured. Security should also cover protection against natural disasters, which can bring big damage, for example storms, floods or extreme temperatures.

b. Integrity Protection tool of network traffic

It is important to keep integrity transferred of data or communication by usage of Demilitarized Zone (DMZ), protection of inner and outer communication perimeter, using cryptography tools and to block unwanted traffic. One of the best practice is network segmentation to smaller individual parts and ensure their security or protection.

c. User Authentication tool

Identity management has to be used to administrate user's database and based on given rules and credentials allow their entrance to system. Each user should have defined privileges only to system he needs or it can be simplified by adding him to group distribution. General rules or best practice for passwords should be used (8 characters, different set of characters, using different password all the time, stronger passwords for administrators and validity for 100 days). Different tools can be used, but the principle must be same and with same results.

d. Access Management tool

Users should have privileges only for usage of applications they need for work and work with data should be protected by set of rules for reading, writing or executing. The CII has to keep information about access to systems in logs.

e. Malicious code protection tool

By Malicious code is understood each code, which should not be in a program and is sending data or information without user's knowing. It is really dangerous and detection tools must be used. The antivirus tool can be able to verify and inspect communication between inner and outer perimeter, servers and data centres, work stations and periodically update own signature threat database.

f. Activity recording tool of users and administrators of CII and SIS:

By law should be logs, flows or any information about activity in system or network stored and archived. The log should contain information about logged user, current time, log–in and log–out time, alerts, activities done during being logged and specially focus on all privilege changes. Important part is to log information of privileged users, such as administrators and their activities, since they can commit attacks with fatal impact. Synchronization of data should be done at least once per day and archived for minimum 3 months.

g. Cyber security Incidents Detection tool

The tool should detect possible malicious behaviour within the network and must be also able to block it. It has to be done for traffic between inner network and dedicated servers. Block

transferred data plays a key aspect to stop the possible attack/incident. It case of CII it should include blocking of internal communication or group of servers.

h. Cyber security Incidents Collecting and Evaluating tool

Based on detection, the information about possible security incident has to be stored for future forensic, mostly done by the security roles. Security policy has to include who and how can work with this tool, since these data give essential information for future improvement of configuration and applied rules or tool's optimization.

i. Application Security

It is common to run at least one web or mobile application and as a result must be used protection tool. This testing has to be done before release and best during development as a part of development cycle. Any code showing malicious behaviour should be rejected and returned to developers for fixing. However it is not only the application itself but it is as well about storing the created code and keeping it in safe storage. Suspicious behaviour coming from outer networks should be protected against unwanted data transfer, changes, wrong transferring or any other data work.

j. Cryptographic Means

Sensitive data or information has to be encrypted to keep its confidentiality and integrity. Administrator is responsible for using some cryptography tool/algorithm. Some hash, symmetric or asymmetric algorithms must be used for transfer or storing of data. All information has to be in Security policy. It includes key–life cycle policy and minimal requirements on used algorithms.

k. High Availability tool

Each key application has to be kept available at least in some limited way for backup and control. Critical network elements should be redundant and designed to be maintained within a specific time frame. In general there should not be any single point of failure implementation, since every necessary elements must be redundant.

l. Security of Industrial and Control Systems

These systems can be called as a SCADA systems, which stands for Supervisory Control and Data Acquisition. They are mostly used in industry as Programmable Logic Controller (PLC). By SCADA is understood control system. These systems can be found in power plants, communication networks or water supply system. From this title it is obligatory to limit people access, remote access, protect against known exploits and to restore their functionality to normal level as soon as possible after an incident is over. In case an attack occurs, there should be a scenario how to handle this incident. The role of Incident manager has to minimize possible impact and is introduced in following chapter.

3.1.2 Paragraph 8

This paragraph mentions Cyber security incident reporting and gives information about organs who must follow the instruction of Cyber security law and their duty to report incidents as soon as any incident occurs. The key information for this thesis is to whom are sent the information and who has the duty of incident reporting. For reporting is used "Incident survey" where is described type of incident and its technical parameters. Unfortunately sometimes it is unclear, if only Cyber–attacks should be reported or other incidents as well.

Reports must be sent to National CERT by:

Authority or person which belongs to Significant Network (in case there is not an administrator of Communication System or Critical Information Infrastructure) with incident report to the National CERT which has signed a memorandum which NSA.

Reports must be sent to Government CERT by:

An administrator of Information System of CII, administrator of Communication or Information System of CII and administrator of SIS report incidents directly to National Cyber security Centre (NCSC) which is part of NSA and is under state control. The main goal of this centre is to operate Government CERT, collaborate with Czech and international CERT/CSIRT teams and to develop Cyber security strategy for future years. In addition, they gather data for incident database and should recommend solutions in case of an attack on public CII or SIS [2].

As a result of this information the thesis is focused in future chapters on public CERT/CSIRT teams and their structure, is presented procedure how to become one of a CERT team and are mentioned two main organizations grouping worldwide CERTs. It is well known how works the National and Government CERT, however private CERT teams can be of use during incidents and are often invited for collaboration. The private CERT should offer services to public. In addition, being a CERT team has an advantage in joining FENIX project, which is a creation of "safe" VLAN, this means that all members will not have a connectivity issue during a big attack on infrastructure. It can be said, that more systems join the FENIX project, less connectivity issue due to an attack will be.

3.2 Regulation 315/2014 Coll.

This regulation is update of Regulation 432/2010 and defines criteria for Critical Information Infrastructure. The criteria are divided into sections based on the branch of business and severity:

- Energetics
  - Electricity
  - Gas
  - Oil and oil products
  - Central Heat supply
- Water resource management
- Food and Agriculture
  - Crop production
  - Livestock production
  - Food production
- Healthcare
- Transit
  - Road transit
  - Rail transit
  - Air transit
  - Interstate water transit
- Communication and Information Systems
  - Technological elements of fixed electronic network communication
  - Technological elements of mobile electronic network communication

    - Technological elements of broadcasting
    - Technological elements of satellite communication
    - Technological elements of post communication
    - Technological elements of information systems
    - **Cyber security domain**
- Financial market and currency
- Emergency services
    - Integrated Rescue Corps
    - Radiation monitoring
    - Forecasting and warning services
- Public administration
    - Public finance
    - Social protection and employment
    - Other public administration
    - Intelligence services

For all these areas are given specific parameters and when they satisfy them, they belong to Critical Information Infrastructure. As it can be seen, these are the fundamental services for running of state and have to be respected, supported and secured accordingly. There is no public list, which organizations belong to Critical Information Infrastructure since it is really sensitive topic and each state is seriously protecting this information.

For this thesis is important to specify criteria how to classify Critical Information Infrastructure as it is written in Cyber security domain. They are as following:

a. Information System which significantly or completely involves activity of specific element in Critical Infrastructure and which is replaceable only after usage of indirect costs or in time frame longer than 8 hours
b. Communication System which significantly or completely involves activity of specific element in Critical Infrastructure and which is replaceable only after usage of indirect costs or in time frame longer than 8 hours.
c. Information system administrated by Public Authority containing personal information about more than 300 000 people.
d. Communication System ensuring connectivity or connection of Critical Infrastructure element with granted data speed at least 1 Gbit/s.
e. Sectoral criteria for determination of Critical Infrastructure element mentioned in a–d are used proportionately for Cyber security domain, unless is element security fulfilling mentioned criteria essential for ensuring Cyber security [1].

These criteria give an overview, how are important for smooth run of state. In next chapters is described, which roles should be in each organization belonging to CII.

3.3 Regulation 316/2014 Coll.

Regulation 316 is the most important for the Cyber security law and because of that is called Cyber security regulation. Specification are shown in paragraph 3.1. Even though Paragraph 5 in Cyber security law covers only information, it was good to mention information from the Cyber security regulation to keep the consistency of the text.

In general regulation is divided into 6 parts:

1. Introductory provisions – § 1 Subject Matter and § 2 Definitions, it is similar to Cyber security law.
2. Security measures – same structure as in Cyber security law with detailed description.
    a. §3 –15: **Organizational measures**
    b. §16 –27: **Technical measures**
    c. §28 and 29: Security Documentation and Certification
3. Cyber security incident – types based on source and possible impact.
4. Reactive measures and Contact information – includes three categories of severity.
5. Effectiveness – since 1 January 2015.
6. Appendixes – in total 7. Third covers Algorithms requirements, 5–7 are forms of survey. Other are mentioned in text below [2].

In Security Documentation should be included map of relations among security countermeasures mentioned in paragraphs 3–27 (Organizational and Technical measures). Records must be easy to understand and cover all security aspects. More details are in Appendixes 1, 2, which cover severity for Risk analysis and evaluation of Assets and 4, which covers possible structure of the Documentation. Documentation structure for CII and SIS has different structure but it is not scope of this thesis.

As is mentioned at the beginning, Cyber security law is mostly using information from ISO/IEC family 27000. CII and SIS, which is certified by ISO/IEC 27001 has to include in documentation scope of their ISMS, its certificate 27001, Cyber security policy and targets, describe methodology used for evaluation of assets and Risk analysis, audit reports and revaluation of inputs and outputs to the system.

3.4 Regulation 317/2014 Coll.

This regulation plays an important role for specifying Significant Information System and their criteria. There are two basic categories – impact and area/district.

Impact criteria are divided into:

1. Complete or partial non–functionality of the system because of security information disruption can have a negative effect on:
    a. Public Authority.
    b. Providing services to public.
    c. Economy of Public Authority which is administrating Significant Information System or Information or Communication Critical Information Infrastructure.
    d. Working of other Significant Information System.
2. Complete or partial non–functionality of the system because of security information disruption can cause:
    a. Threat to element of Critical Information Infrastructure.
    b. More than 10 casualties and over 100 injured with more than 24 hours long hospitalization.
    c. Financial or material loss with marginally value larger than 5% of Public Authority budget.
    d. Impact on 50 000 people.
    e. Significant threat or disruption of public interest.

The values should not exceed the limits specifying the Critical Information Infrastructure. The regional criteria are specified in Appendix 2 of 317/2014. [3]

From the criteria it can be seen, that impacted systems are really of great value, have an effect on many people and can even cause loss of lives. Whole list is in Appendix 1 of 317/2014. However compare to criteria of CII, these are less strict.

At the end it is important to mention, that specifying if the organization should be part of SIS does organization itself, after proposing to National or Government CERT (depends on the institution) audit will be done to confirm the proposal. In case that proposal is positive, the organization can be called as a member of Significant Information System and has to fulfil all given duties of it. On the other hand when National or Government CERT finds out that organization belongs to Significant Information System and did not inform about it, no penalty or other sanction is given and the organization has to proceed with regular steps.

Three key duties are:

1. Within 30 days send a Survey with contact information (Appendix 7 of 316/2014 Coll.)
2. Within 12 months implement security measures.
3. After 12 months report incidents and prepare for NSA audit.

These duties are really strict and some of the deadlines are impossible to satisfy. First duty is quite easy and can be satisfied on time, since in almost every SIS should be some security department and to give contact information, does not take so much time.

However problem comes with the second duty. As is described, the systems are usually really big, they have complex infrastructure which is decentralized around the Czech Republic. In some cases implementation of security elements is not as difficult, however as it was mentioned, it is not only about security element, it has to come with Security policy, which limits labours. For good policy and hardware implementation has to be done an analysis, which usually takes long time due to complexity and severity of the system. Finally when is analysis done, security elements can be bought as are proposed in the analysis. Nevertheless, buying a new equipment in public organization is not an easy task. Since implementation, tools and analysis are costly has to be listed for everything a tender. It is not an issue, that tender can be listed for limited time period, however a problem is to write the tender well, so the proposed solution is chosen. Based on a law 137/2006 about public procurement, has to be chosen the procurement with the lowest price, which is not always the best solution or is not even recommendation of the analysis and might be insufficient. Next problem is when the solution is chosen well, however some other competitor is not satisfied with the result and decides to appeal to a higher authority. This means stoppage of implementation and all the progress, since it must be allowed to an appeal and relevant authorities will decide if the appeal is authorized or not. However in some cases this can slow down whole process for months (in good cases) but mostly for years.

Point three is an audit, which controls the duties based on organizational and technical measures. In case something is missing, the process goes back second to point and has to be implemented.

As a result can be seen, how bureaucracy slowdowns improvement and security measures, where years of waiting can have fatal impact on the organization work.

4 Cyber security roles

So far it was discussed which legislative regulation are key for Cyber security and its specification. The most important is Cyber security law (181/2014 Coll.) and Cyber security regulation (316/2014 Coll.). Moreover, it was discussed how important is to satisfy Organizational and Technical measures, which are closely introduced, too. This chapter is focused on 181/2014, § 5 Organizational Security which defines roles. All roles should have at least 3 year experience with their focus – for example Architect should have been for 3 years architect of information security [4]. The Steering committee is not scope of this thesis.

However Incident Manager and CERT team are not mentioned in that paragraph, even though they are discussed, since they play significant role it Cyber security defence and incident handling.

4.1 CERT/CSIRT

As was mentioned first team was established at the Carnegie Mellon University in 1988. In the Czech Republic is the history much shorter and so far there are two public CERT teams, one on National level – CZ.NIC and second on Government level – GOVCERT (part of National Cyber security Centre). However these two are not the only CERTs in the Czech Republic and worldwide can be found many more of them, but not each of them has a good results. The relation between public and private CERT is in Figure 4.1, where it can be seen, that public CERT are controlled by NSA, however private CERT can be invited or asked for help during an incident.

Good reviews and very active in Czech are these teams: ACTIVE24–CSIRT, CESNET–CERTS, and CSIRT–MU. Lastly mentioned is CSIRT at Masaryk University in Brno, where was established Cybernetic Polygon and is the only Certified team in Czech [13]. For becoming a private CERT/CSIRT you have to fulfil several conditions, which are difficult to follow.

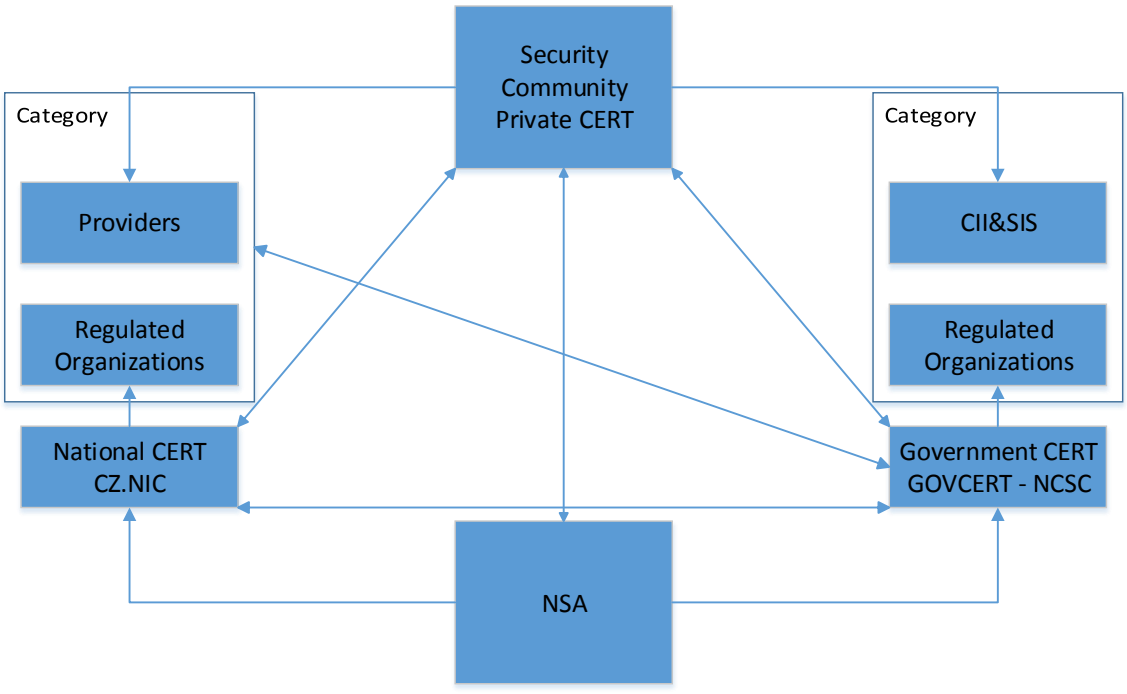


Figure 4.1 Relation among Private&Public CERT

The process of becoming a certified CERT team is quite complex. For example Trusted Introducer (TI), which was established at beginning of new millennium for the European Union has 3 stages [13]:

- Listed – shows acceptance to Trusted Introducer (TI) community and brief information about the team itself.
- Accredited – shows fulfilling of the TI processes and improvement in applying gain experience to practice.
- Certified – the highest level which shows level of skills and know–how, which can be shared with other teams.

To become "Listed" it is good to have at least two recommendations from other CERT/CSIRT teams, which ensure your skill. During the application other members can show their concerns about entering to TI Community. Moreover, the new coming CERT has to choose which Services it wants to offer. Three basic categories are shown Figure 4.2 and are described as [16]:

- Reactive Services – when an incident or an event occurs, these services have a key role in handling of malicious code attack, system penetration, exploit detection or other threats.
- Proactive Services – help to minimalize the attack impact with improvement of technological measures and can decrease the possible effect of future events.
- Security Quality Management Services – they cover the development and improvement of organizational measures, since they play significant role in Cyber security. As is known, the chain is as strong as his weakest part and in these days it is a human.

The CERT has to provide or cover at least one of Incident Handling service – incident analysis, incident response on site, incident response support or incident response coordination, otherwise cannot get a status "Listed". However these are minimum requirements and for better reputation and quality of the team it is important to cover more categories. It is necessary to mention, that each organization covers the costs from own resources.

In case of "Accredited", you have to be firstly listed, afterwards it takes maximum 4 months to be accredited, if you meet given criteria, which are complex and are similar to §5 Organizational and Technical measures, as well as all information about team members, their qualification should be given, since they have to keep sensitive data. Key role play list of offered services regards to Figure 4.2.

Last case is "Certified", which is the most difficult and requires audit and evaluation of 4 categories:

1. Organisation
2. Human
3. Tools
4. Processes

These categories have in total 45 parameters, which are graded and base on that is created a Quadrant model. Proprietary SIM3 Model methodology is used for that.[16]

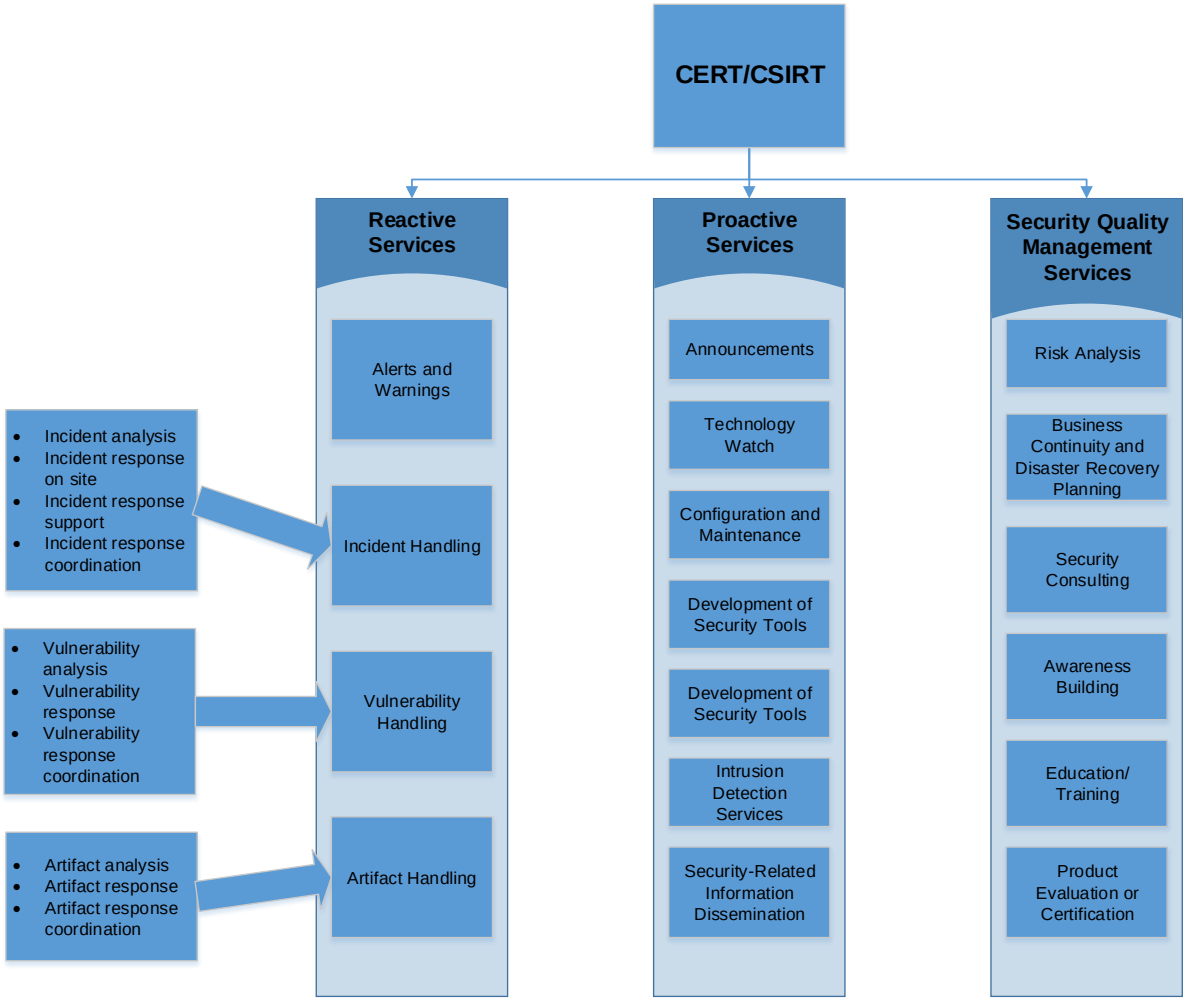


Figure 4.2 CERT Services

The best practise for being a good CERT team is to base your work on 3 or in some cases 4 key activities:

1. Gathering and evaluation of information resources – it is important, since if you want to face an incident, you have to know which attack it is. The work of CERT is based on collaboration and due diligence, since Cyber space is worldwide. These information can be found in:
    a. Database – CISCO PSIRT, IBM X–Force or some other big names have own teams, which are gathering information and signatures of attacks in real–time. They offer this database, however it is not always free of charge. These signatures can be stored within their own Security devices, like SIEM, IPS, or Firewall and is up–to date.
    b. Sharing information about incidents with other CERT teams is common in practise. For example if your organization is under an Cyber–attack and you do not know how to handle it, you can ask other teams for help, however you have to consider sharing sensitive data. This decision is up to an Incident manager, which is introduced in next chapter.
2. Security incident response plan –security plans preparation what to do in case of an attack → Identify, Analyse, Act. Tools or resources for these plans are:
    a. Risk analysis – comparing possible impact and evaluation of assets

   b. Continuity management – identify and ensure minimal level of system availability by making a list of key services
3. Post incident services – detailed analysis how the attack happened, basically it is a forensic work: how did the attacker penetrate and ensure that this vulnerability will not be used again. The report can be used as a material for criminal act.
4. War games/Cyber combat, vulnerability test (automatic), penetration tests (manual) – some teams offer own system of training and evaluation of Human resources. The tool for that are specific workshops, where are simulated attacks in real–time. This can be done in two ways:
   a. Technical background – where is used expensive hardware on specific scenario, example of this can Cybernetic polygon (Brno, CyberGym, Estonia). These are really interesting tools, however it is costly and only few companies can effort it. Information are gathered before the workshop to prepare specific scenario, which can also occur during normal run. Nevertheless it is difficult to modify the Hardware in polygon infrastructure to be the same like the "real" infrastructure of the company.
   b. Table top – mostly used with analysis, less detail on real–time attacks and its defence. Detailed analysis is done before to meet specific requirements.

Both approaches improve the knowledge and skill of tested persons or systems, however pros and cons have to be taken into account, especially price vs specialization.

Opposite of the vulnerability test, which are done by automated tools are the manual penetration tests. From this can be seen, that penetration tests require more resources, since only experienced human is capable of that. These tests have to be discussed with management and introduced to security department of involved organization.

Second main institution regards to CERT/CSIRT is group FIRST (Forum of Incident Response and Security Teams) [23] which covers the US teams. Significant CERT/CSIRT teams are members in both organizations. They have regular meetings where are discussed current issues.

At the end it is important to mention, that teams have great know–how and base on the networking among teams they are capable of many things, however this know–how has to be transformed into processes and possible vector of an attack. The teams have to be active and if they have good know–how, their services will be used, which can bring benefits to them.

4.2 Manager

Manager is the first mentioned role in the Cyber security law. His responsibilities are wide and has to fulfil basic technical and especially organizational skills. His work is focused on a "topology" as shown in Figure 4.3. He approaches to the topology from the top, since his attitude has to be market oriented with keeping the own network secure. He has to work closely with his team members – architect, asset administrators and others specialist to ensure that the network is running well and business is not in danger. Since Cyber security is not only matter of technical equipment, but in addition bigger portion of processes and Security policy. Manager has to be few steps ahead of implementation to new technology and know the possible impact on the company.

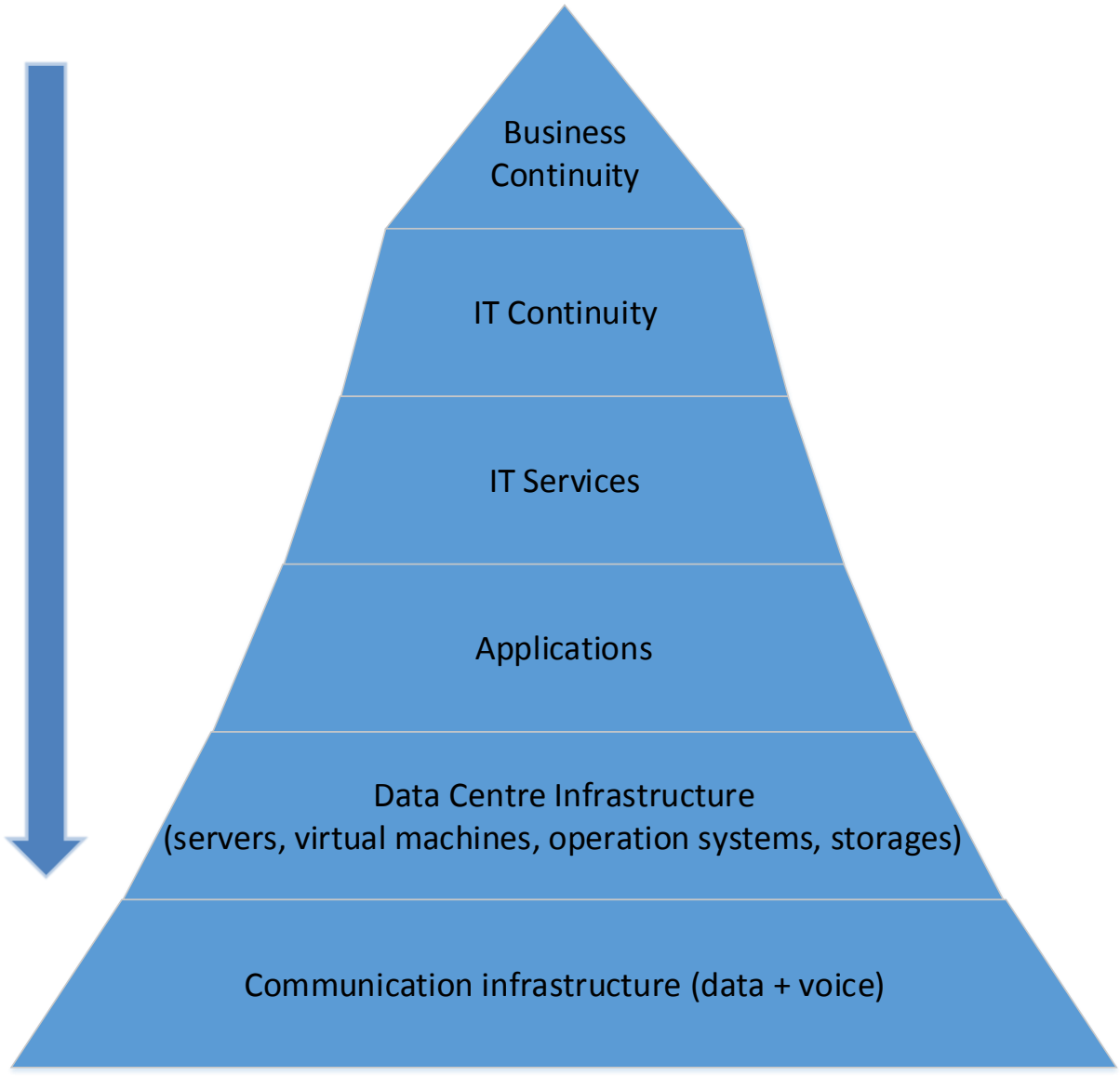


Figure 4.3 Manager's "topology“

Key steps to ensure stability of system are:

1. To define scope of the system – requires know–how of the network and has to be done in collaboration with an Architect, deep knowledge of the business infrastructure, creation of new documentation – policy, methodology or inner regulations.
2. Analysis and evaluation of assets – requires knowledge of business. Information can be gain from Control department, Sales department or Legal department. These departments know the financial value of assets, which might be for some companies the key indicator, however other aspects play an important role.
3. Risk analysis and management – requires good technical knowledge, since it has to ask for detailed subjects of infrastructure and answer its weak spots.
4. Implementation of countermeasures – can be done as security policy – processes, documentation or technical measures, which leads to investment in new Hardware.
5. Evaluation of ISMS security – these things has to be done continuously, since threats are evolving as well and the defence has to go in hand.

In Figure 4.3, can be seen what is the most important aspect is for the Manager – Business Continuity Management. More information about it is possible to find in ISO/IEC 27031 [14], where are guidelines for information and communication technology readiness for business continuity and ISO/IEC 22301 [15], where are described requirements which belongs to the organizational part.

By Business Continuity Management (BCM) is meant a set of planning, preparations and countermeasure activities to ensure that the business is running even when an incident happens. The scope of business covers the critical (key) business functionalities how to ensure their run. The set of rules can be described by three factors:

- Resilience or incident preparedness – the infrastructure is designed in resilient way, which can be for example using of High Availability (HA), duplication of system to other geographical location (decentralization) or having independent parts of infrastructure.
- Recovery plan – in case of an incident follows a plan which helps to run primary and secondary functions of the company. For this is important good metric for asset evaluation.
- Contingency or Emergency response management – in case of an attack, someone has to take the lead with set of responsibilities. This person is called an Incident Manager and is described in following chapter.

It can be understood as a thinking about a threat, which is actually a vulnerability of the system, which can have an impact to Confidentiality, Integrity and Availability (CIA) of our system and data. Moreover, part of BCM is Change Management and other factors mentioned in paragraph 5 of Organizational countermeasures.

Second to discuss is the IT Continuity which is a subset of BCM and is focused on the IT continuity planning. In addition, it covers communication infrastructure capabilities of handling data and voice transfer. It is a regulated process of preventing, predicting and managing incidents which may occur in IT and have potentially bad effect on IT Services.

Third one in hierarchy are IT Services. Most employees are working with some service and it can vary from billing to card entrance system. In case the service does not work, end users are the first one who realize. In general it is possible to say, they do not care where the service runs (which server or location), through which path the data flow but they care the availability. It is work of an Asset Administrator, an Architect and the Manager to ensure the service run. Besides the evaluation should be part of Risk analysis and Risk management.

After that are the Applications, which can be understood as a piece of Software (program or Operating system) used for work. It is similar and closely connected with IT Services. It is mentioned in the regulation how to work with the application to ensure maximum benefit in combination with security. It is up to the Asset Administrator to take care about it – updating, checking malicious behaviour and offer it to the end user.

Next point are Data Centres. Data Centres have a key aspect in ensuring CIA and with application can be target of an attack and also help to block it. In general manager has the knowledge by which services it is used and what applications are running on it, however his deeper knowledge about which assets does it use is out of his scope. He cannot cover and look after it, though he should have documentation and basic understanding of the functionality and know who is responsible for the smooth run. He needs these information for making a good Risk analysis and to keep it up to date.

Last one is Communication infrastructure, which is the connection of the physical topology with the Software running over it. It has to keep CIA as well, since usage of safe protocols for

transfer, continuous monitoring and detecting of possible breaches has to be ensured. For example having Dual–multi–homed connectivity or encrypted data transfer.

From the Figure 4.4 it is possible to see, that Manager is using on daily base PDCA cycle, which was mentioned in previous chapter.

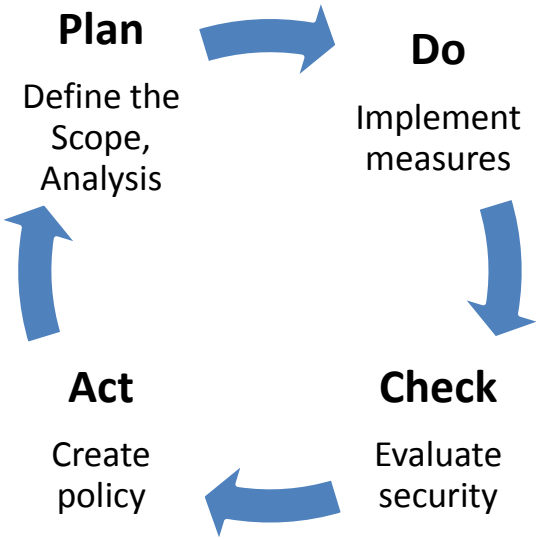


Figure 4.4 PDCA - Manager

Manager has the difficult task to try to apply the policies (can be really difficult in big or small companies, since many people do not see the reason why to change something). Next point is to find budget, since Security department does not generate income and is really costly. Furthermore, he has to set a strategy for future development and communicate with top managers to get their financial and power support. Fortunately for Manager, research and many incidents has been made, which show possible impact if you do not invest to infrastructure. However getting support is not enough, since biggest threat for the network are the employees and most of the Security policy restrict or limits their activities and applying the policy is not an easy task.

Generally saying firstly has to be generated policy (organizational measure) before any technical equipment is bought, since if you do not have good plan or project, your technical equipment might be just an obstacle. Manager has to decide it and create such policy. Top management has to know about the plans, since they have the responsibility for that and will have to report (in case of CII or SIS) to Government.

It is important to realize, that the Manager has to choose very carefully also the supplier of security solutions or in general the third site parties, since they know the company from inside.

Figure 4.5 Knowledge vs Specialization "T" profile - Manager

It goes in head with signing Service Level Agreements (SLAs), Non–Disclosure Agreements (NDAs) and in some cases the vendors have to fulfil different levels of Certification.

As a result the Manager should have good legislative and technical knowledge, be flexible and stress resistant, additionally should have good communication skills. His profile can be graphically shown as an inverted T letter, Figure 4.5, he should have wide knowledge base with narrow specialization, which usually comes from his previous field. He has to be experienced in networking and with gained experience from the field suggest future ways.

4.3 Architect

So far it was discussed how Manager works and as it is known from Paragraph 5, he is mostly responsible for Organizational actions, on the other hand is an Architect, who is specializing on the technical measures. This is not an easy task, since there are plenty of solution how to do it and most of them are really costly. The financial issue has to be presented to the Manager who will go to Top Management and warrant these steps. In case of CII or SIS, they have to fulfil technical solutions regards to regulation 316/2014 [2]. From this it can be seen, that Architect has to be more technically oriented and be a specialist in security elements. Basically saying he should have been an implementer of security solutions, with long experience before he can become the Architect, where is he combining all his previous knowledge with more responsibility and covering as well legislative recommendations.

These steps can be described like this – firstly think, after act, which means you have to make a good analysis, covering all the aspects (behaviour of employees, process life cycle, checking and improvement….). When processes are done, implementation can start, since usually implementation itself is less violent to company run compare to process changes. As is known, labours are the biggest threat to the network and if they do not use the technology well or do not respect the rules, they will bypass it and create possible security holes.

His profile can be described as is shown in Figure 4.6. Where on Knowledge axis is covered organization topology and current processes and on Specialization axis are hidden security elements, attacks and their counterattacks and many more. There is significant difference between Manager and Architect approaching to the problem, however they have to find the way to collaborate, since they have common target.

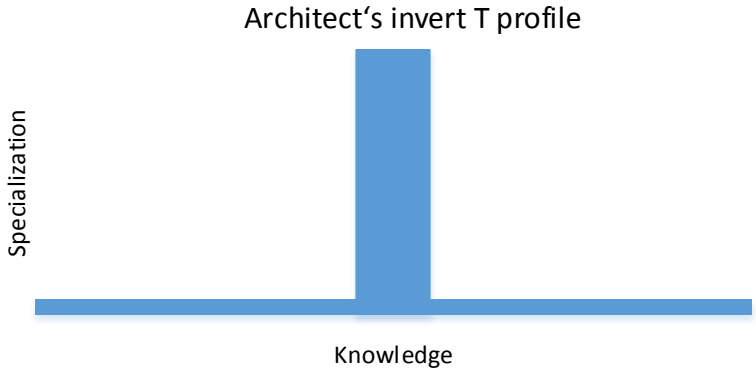


Figure 4.6 Knowledge vs Specialization “T” profile - Architect

When it is taken a look at Technical measures, there is mentioned physical security, application security, access management, incidents or events detection, logging and storage of information and evaluation of stored data and to keep continuity. These facts are representing ISO/ISO networking model with its 7 layers and mostly its second (Data Link) and third

(Network) layer. Based on this fact, was created a Figure 4.7, which can be understood as basic Architect's topology, covering all technical measures.

Firstly it is important to understand what each device is and briefly describe how it works, before flows in topology are explained. Here is given brief explanation about security elements.

- Intrusion Detection System (IDS)/ Intrusion Prevention System (IPS) – IDS is detecting traffic and analysing based on given rules IP, PORT and Payload of packets. In case it finds a malicious traffic/content it alarms the operator, on the other hand IPS blocks/rejects this traffic.
- Next Generation IPS/IDS – is covering 7 layer (Application) of traffic, this is done by looking into content. Some other features can be decryption of traffic in real time, since malicious content would be otherwise out of sign. Other feature can be behavioural analysis of malware.
- Firewall – comparing to IDS/IPS firewall is just comparing IP address and ports based on rules. It can be said Firewall just discards traffic based on rules.
- Next Generation Firewall – modern Firewalls are covering within their features IDS/IPS, behavioural controls, decryption of encrypted traffic, regular updates from common black lists authorities or content signatures analysis and many more.
- Security Information Event Management (SIEM) – SIEM is a passive security tool collecting information (Logs and Flows) from other security elements or servers within infrastructure. These data are correlated and based on given rules are shown alarms or false positives. The gathered data can be stored for future analysis (forensic or as an evidence of an incident). This tool is understood as a base of Security Intelligence.
- Identity and Access Management (IAM) – is a centralized system of users' credentials and based on that assigning required resources. These tools are capable of keeping password life cycles, work with physical security (entrance cards, tokens) or Workflows. This tool keeps up–to date track of users.
- Application/Vulnerability Scanners – these tools are used for detection of malicious behaviour in application by running it in Black box (simulation of user's behaviour) or White box (code control and its flow).
- Endpoint Controller – Controller on endpoint station and its status; if antivirus, system and programs are up to date, no unknown software is installed, Hard Drive is encrypted, and there are not unknown signatures within the system. Moreover, it can cover control of Mobile Devices and its tracking and erasing of sensitive data from distance.
- Log file – event recording file storing information about logging into system, work at there, shared communication among users. This log format consists of time, user's ID, IP and some other information.
- Flow – continuous collection of packets giving us information about IP addresses, ports, type of service and Simple Network Management Protocol (SNMP). Basically saying it is giving overview of traffic and is key for its analysis.
- High Availability (HA) – redundant solution of HW, to avoid single point of failure issue and to ensure continuity and availability of system.

From this can be seen, we need an Asset Administrator/operator who looks after the devices to update their rules, respond to possible detection and is all the time optimizing these security systems. In case the administrator does not have competence, the tool is useless.

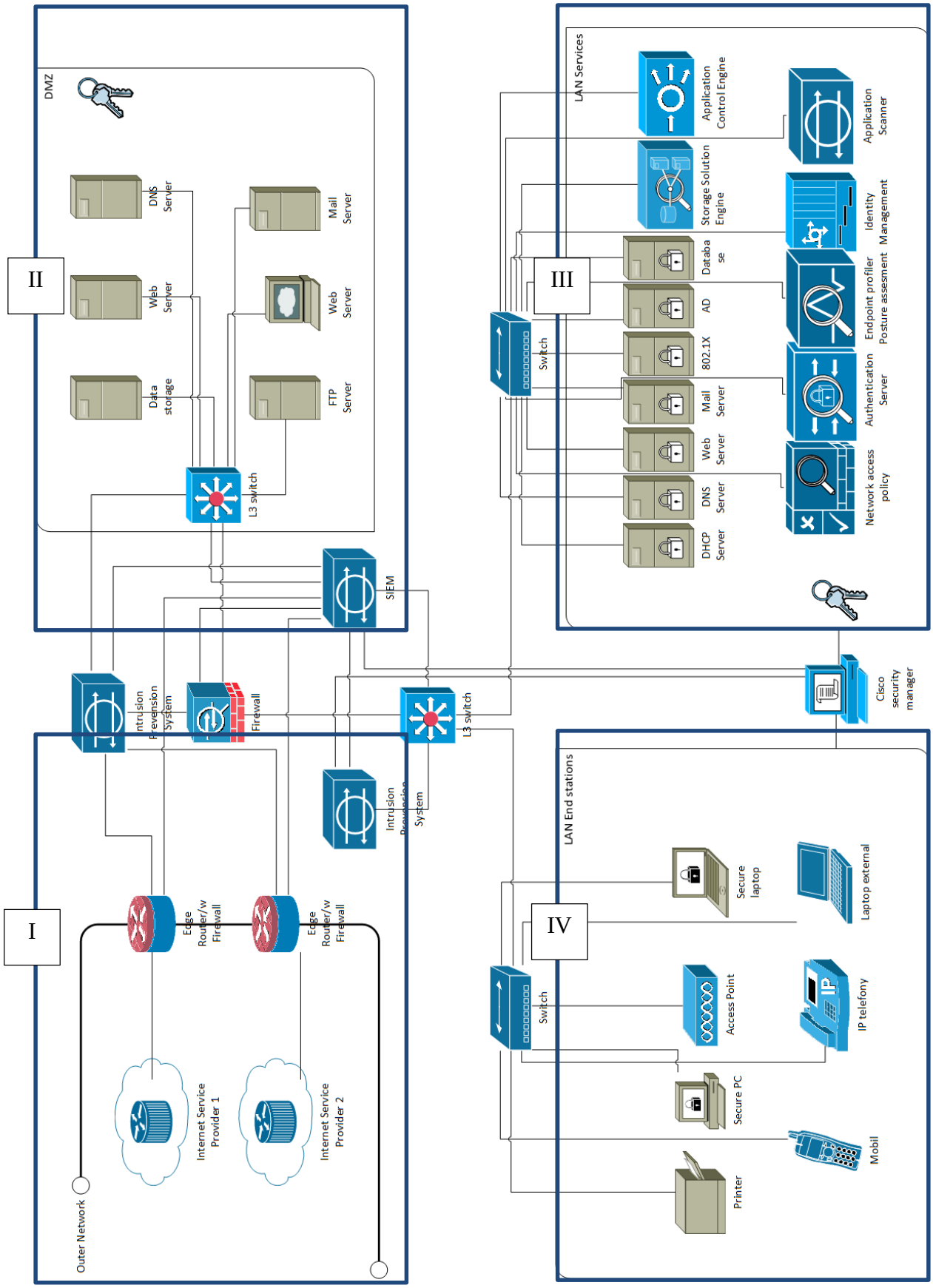


Figure 4.7 Architect's topology

So far it was discussed which basic security elements are important for an architect and how do they work. It this part is described closely his topology, which is divided into 4 sections – Outer network, DMZ, LAN Services and LAN.

First Section is the connection to the Internet and outer world. Internet is provided Multi homed, which means the infrastructure has two different Internet Service Providers (ISP) in case one link collapses. The redundancy is in addition on the site of Gateway, where are two routers. By this redundancy is completely eliminated single point of failure. In case of even better solution can be these Gateways in geographically different areas. By connection to the Internet, our infrastructure becomes vulnerable from outside, because of that are several defence mechanism used. First one is Hardware central Firewall and two Software firewalls on Edge routers. For the security reasons things like NAT (Network Address Translation) or Proxy are used to differ between outer and inner network. Besides all the traffic going in and out is controlled by IPS.

Second Section is called DMZ. In this zone are services offered to public and to inner labours, such as Web browsing, Email, Domain Name System (DNS) or Data storages. The outer user does not have the IP address, since all the addresses are translated on Edge routers. The connectivity is provided through Layer 3 Switch to ensure Integrity by checksums of data. The HA solution can be provided for maximum Availability. As is shown in the picture, the "Key" symbolizes that all the traffic is encrypted to ensure Confidentiality of transferred data.

Third section is sensitive to administration of our Inner network, since it conducts all the management services, private servers and databases. For management are used IAM, Network access policy, Authentication Server (AAA – Authentication, Authorization and Accounting Server, such as TACACS or Radius) and Endpoint profiler. IAM is defining the Authorization (giving resources to defined roles) and keeps Authentication information (credentials). However the act of login is done through AAA Server. These three are together offering a solution to cover 802.1X Standard. It is used for dynamically assigning virtual LAN (VLAN) to an endpoints which want to have connectivity to the infrastructure. So every RJ–45 slot or Wireless session before the PC is connected has to login with credential and based on IAM are assigned specific VLANs, which the end user might need for work. Private servers can be Active Directory (AD), DHCP, Storages, Application scanners or servers to host some applications (Web, DNS …). Last section are database servers, which have different vulnerabilities and are storing sensitive data, because of that must be well cared and protected. This can be done by encryption mechanism, strict edit policy and many more.

Fourth section are all the endpoints – private or public phones, laptops, printers, fax, access point (AP), tablets and others. In case of public – company given accessories, it is easier, since they are connected and administrated. Many plug–ins to check their content can be done and by using antiviruses, legal software and 802.1X it is safer. However private things bring more threats, since it is not known what Software is in them, here is 802.1X a must. The policy for private accessories has to be done even though it brings many complains. Current issue is Bring Your Own Device (BYOD), since employees want to be use their private phones or tablets. Mobility management solution has to be offered, otherwise people will find the way to bypass it.

Last section is everything what is not inside any of the previous sections. This can be Security Management, SIEM, some switches and wires. Security Management is used for monitoring and it can for example Supervision centre, where is seen if everything is working well. SIEM is gathering and correlating all the Logs and Flows from the network and in case of big networks we are talking about hundred thousands of flows and logs, since almost every

Server, Firewall, IPS or Router is generating them. As a result SIEM has to powerful HW tool, with enough storage to keep all the data for evaluation. Next issue are Virtual Private Network (VPN), which bring possible threats and have to be offered only in case of need.

All the servers and services have in common to keep CIA, it can be done by HA, geographical distribution, having spare parts to immediate repair or SLA with service, never ending encrypting, periodical back–ups and its content controls. Each section has different types of threats, nevertheless Architect has to think about "Big picture" and secure the network. Furthermore, he should cover Application life–cycle and collaborate with development department. Next step is certification authority for valid security certification used in communication.

His next duty is to care about Physical Security. This covers CCTV, Access Management (cards, tokens), Electronic security alarm, fire security, backup power supply (UPS, diesel), protection against mechanical damage and even Air condition to keep optional conditions for run of components.

In summary the Architect is defining the security of infrastructure and has to be all the time up to date of possible threats and try to prepare protection against them. He needs to have a good team which is capable of administration or as well implementation of each security mechanisms. In addition, he should cover the SCADA systems security in industry areas, which is next difficult task, but is out of the scope of this thesis.

4.4 Auditor

In general Audit serves to check or control status of company and evaluation. Audit has to be done by independent person, without hidden relation to the audited organization. There are different types Audits – accounting, assessments, integrated studies, forensic audits and for the scope of this thesis security audit. Auditor role is really important, since company needs to be evaluated. There are several reasons why to do it, for example to get certification of ISO/IEC 27000, which can be important to take part in public tenders, other reason to ensure trust of investors.

There are two basic types of audit – internal and external. Internal is focused on evaluation of processes and external focused on accounting evaluation. It is possible to understand internal as an audit made by own employees and external done by outer company. This thesis is focused on internal Auditor role.

Important standards for auditors are ISO/IEC 19011, which is standard for Guidelines for management systems auditing [5] and for auditing of ISMS it is ISO/IEC 27007 Guidelines for information security management systems auditing [6]. In general Auditor should know such a standard which is required for specific audit. In Czech should be used audit scope described in Cyber security regulation 316/2014 Coll. § 29 Certification. The organization certified by ISO/IEC 27001 must have these documents [2]:

- Define scope of ISMS – which systems, assets and policies or processes.
- Policy statement and strategy of ISMS.
- Description of used methodology for Risk analysis and its result and asset evaluation.
- Statement of Applicability.
- ISO/IEC 27001 ISMS Certificate.
- Report of ISMS evaluation including information about inputs and outputs.

- Report of Audit including records about improvement of shortcomings.

These are the documents, which have to be, when it is thought oppositely – these are the documents Auditor has to check and organization has to be prepared before they want to be audited. The difference between Manager and Auditor can be seen in Figure 4.8 Auditor's approach, where the Auditor approaches to the topology from the site, he cares about each layer independently or in a big picture. The approach depends on the organization and defined scope of audit.

For example he might want to check only few main Services, where it is known they work well, though the other less significant services are not in such a good condition. It is up to the Auditor to give questions and to find possible problems. Giving the company the certificate means a big responsibility for the Auditor and organization he represents. As a result he has to bring evidence of his Audit back to his home organization.

There are several different Auditors experience levels and certification in different specialization (for example ISMS Auditor, Accounting Auditor …), but they have in common that the courses they been through are certified by IRCA (The International Register of

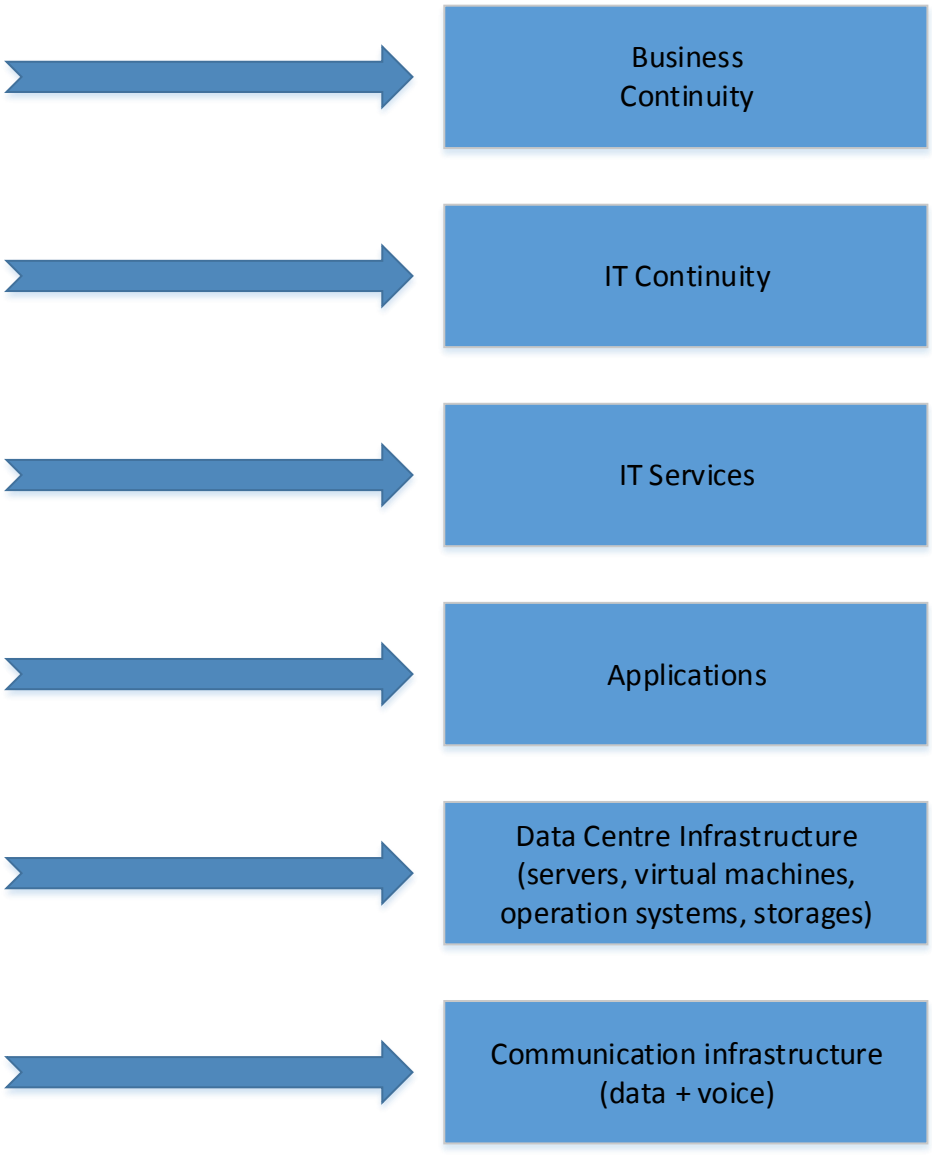


Figure 4.8 Auditor's approach

Certificated Auditors) [17]. This organization is offering solution for personal development and certification of Auditors with impact on experience and hands–on skills.

The Auditors of ISMS can have three roles:

- Team member – auditor team, having many members doing an Audit, can have less experienced and professional within a team.
- Lead Auditor – is a leader of Audit, he is responsible for the audit and for the team he chooses for the audit. He is the most experienced and can be certified by for example Certification authority – IRCA, ITIL and many more…
- Auditor – in some case Auditor can be alone for his specific field and act by his own, usually he has to be experienced by team Audits.

Auditor should have knowledge of ISMS specification and great knowledge of ISO/IEC 27000 for that. Criteria are qualitative (certification) and quantitative (years of experience) [17]. The profile can be seen in Figure 4.9, where is even wider knowledge about legislative and technical issue with smaller specialization to specific audit's needs – like ISMS.

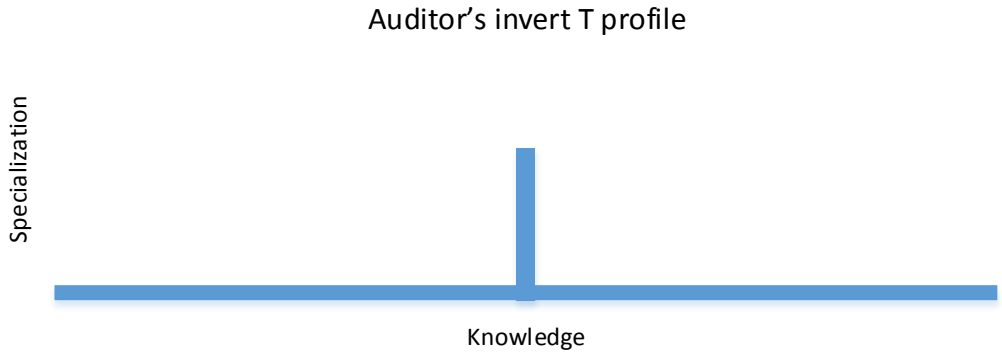


Figure 4.9 Knowledge vs Specialization "T" profile - Auditor

Audit is time demanding and requires a lot of preparation, since the time of Auditor is expensive. Preparation for audit takes weeks or even months depending on the scope. The procedure is described in Figure 4.10, where are defined procedures in PDCA cycle.

Plan part is mostly up to the organization and about Audit has to decide the Top management of the organization, since they are the only one who can define the roles and scope. Set of documents is prepared and is given to Auditors in advance. This is not an easy task and requires experienced people on both sites, otherwise the effect will not come.

Do part is about the action itself. The methodology has to be defined based on the scope and requirements, qualified team has to be chosen and responsibilities given. When the auditors come to company they check in a week pieces of documentation a do brief and random interview with Administrators of defined assets. This is really short period to find possible problems, but they mostly care about used system or methodology than about the details, since it would take too long time. They briefly pick up few samples and store it.

Checking is about periodical improvement, since Audits have to come regularly and usually they check if the absence processes have been improved or how is the progress going. Furthermore, sometimes was not chosen efficient approach and can be improved or scope was not sufficient. These tasks are not easy to evaluate and depends on experience of Auditors.

Lastly **Act**ing means that the organization has to be examined by report, where are or gathered information given and lacks shown. These reports have to be signed, which means they are taken into account and will be part of future improvement. Countermeasures or some action has to be decided. Besides, it can mean that the shortage does not play significant role

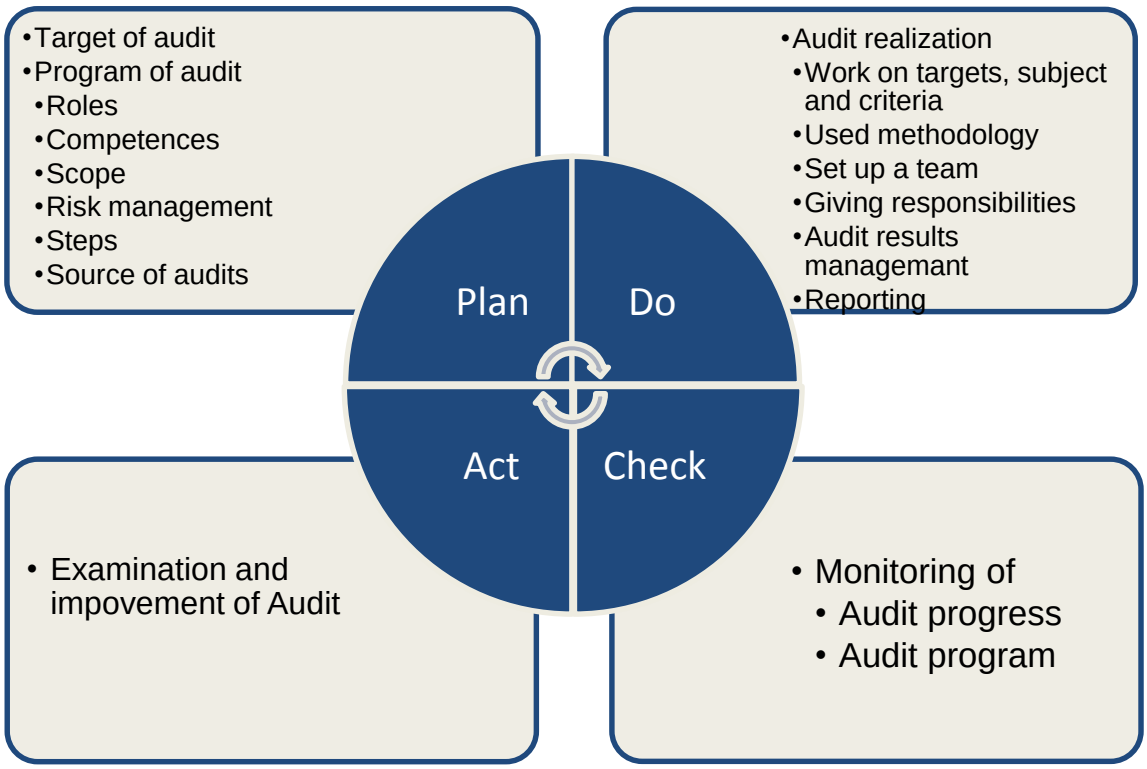


Figure 4.10 PDCA – Auditor

and as a result might not be repaired, nevertheless this decision has to be done, since following Audit will feel suspicious why nothing happened.

At the end, Auditor has a difficult work and has in hand reputation of his home organization and audited organization, because of that he is in never ending improvement and lectures to follow modern approaches. IRCA is giving good personal growth overview and plays an important role in career of each Auditor. Other to mention can be organization ISACA (Information Systems Audit and Control Association), which offers CISA (Certified Information Systems Auditor) [21] system, where is a mandatory to participate on seminars in minimum 20 hours/year to keep the certification.

4.5 Asset Administrator

Administrator has responsibility to look after information asset and ensure its functionality, continuous improvement, which goes in hand with maintenance and security of communication and information system. By asset is understood everything valuable to the company. It can be either primary or subsidiary asset, where primary is intangible (know–how, processes, data, information…) and subsidiary is tangible (employees, suppliers, technical and programming equipment…) which serves to support primary assets.

Admin has to ensure that data and information are kept confidential, integrated and available all the time, since other assets or services are dependent on it.

By confidentiality is meant keeping the data or information in private – no one else than source and destination should know the content, this means that data will not be redirected to wrong people by authorization or in case it happens how to ensure that the content will be unreadable. Technics for that can be encryption by cryptographic algorithms in combination with hash algorithms. The countermeasures depend on the confidentiality level of transported data.

Integrity is maintenance of transported data, which they will be still consistent, trustworthy and content will not be changed without knowing. This can be done by controlling of access (logs, flows) and using prevention or detection mechanism like checksums. It is a big issue in running a program or system and only possible approach how to restore integrity is usage of backup, which has to be regularly checked and be sure CIA is ensured.

Last to mention is availability that connect Hardware and communication channels. Problem can occur even by restarting a system to install updates. It is important to inform about such actions. Availability can be ensured by usage of RAIDs, High Availability (HA) or in general redundancy. Key is to avoid Single points of failure. Recovery plans should be described for many possible scenarios and can consider different geographical locations, backups (caring about them), security elements and many more.

From this it is seen that Administrator should be specialist to single area as is shown in Figure 4.11., the specialization is based on his field of work – Server admin has for example knowledge of Linux distribution, networking, Virtual Machines and ISO/OSI protocols.

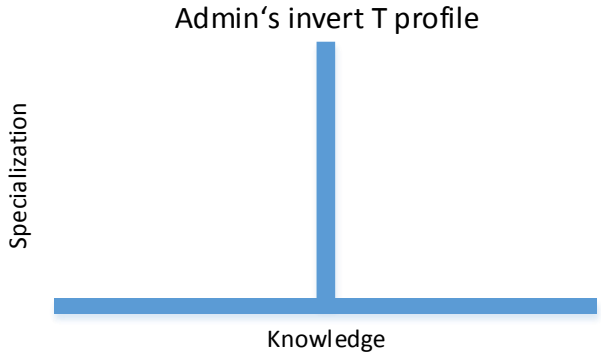


Figure 4.11 Knowledge vs Specialization “T” profile - Administrator

On the other hand his asset (primary know–how is how to administrate, subsidiary the piece of HW), is in the second layer – data centre as is presented in Figure 4.12. Administrator cares about the status of server and one layer below which is communication infrastructure. He should have knowledge about it and be able to troubleshoot it in case of a problem, as well as knowing through which network elements are data directed. Of course he cannot know about everything, but he should know whom to contact in case of a problem and define where is the trouble. From the picture is possible to see he does not have responsibility for upper layers. Nevertheless some administrator of asset above him has to know about it.

In general in case of an issue the problem will bubble to the lowest layer where problem occurs. This means Administrator on top, should know about lower layers, since they are imperishable in the infrastructure and they bear responsibility for that. Usually with this responsibility comes bigger motivation. On the top is Manager and Architect who should know about general functionality but do not know details like configuration.

Moreover, profile of Asset administrator should cover knowledge of legislative – brief information about ISO/IEC and Cyber security law. In addition, his work should respect Security policy created by Manager and should follow best practise use cases. Manager bears the responsibility for this and his tools for checking it is Risk analysis and periodical audit.

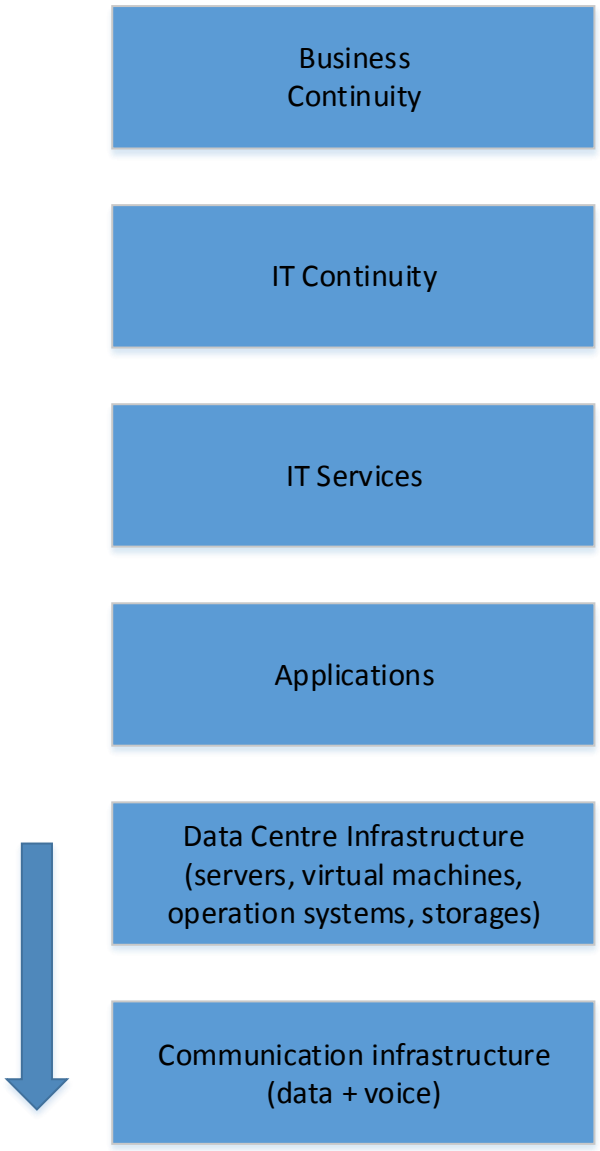


Figure 4.12 Asset Admin problem scope

Furthermore, administrator should be educated to follow trends and be specialist in his field. This invest can lead to securer infrastructure, since misconfiguration can lead to vulnerability and threat to the system.

4.6 Incident Manager

Lastly mentioned is an Incident Manager, even though Cyber security law does not cover this role, he plays a major role in handling of an attack. He is the main authority of Incident Management and can be understood as a Conductor of Incident handling. This role is however described in ITIL v3. He has given several responsibilities:

- Run the team of specialist (System Engineers) to monitor and determine an incident, it can combine Asset Managers and other previously mentioned roles. This team can be distributed and the communication should be only through telephone, since other communication is not fast enough.
- Know and understand an incident to be able to handle it and use sufficient resources.

- Analyse and make wide overview of the incident to track its actions.
- Have knowledge about basic functionality of wide areas like Core Network, Remote access service, Value–added service, Core systems and others.
- Follow scenario to gain network under control again.
- Communication with key customers about the incident and ensure when the service will be online again.
- Everything has to be well reported and used for future improvement.

From this it can be seen he can use all resources organization offers and even more to minimize the impact. He can ask for help of CERT/CSIRT teams, or NSA which gives recommendation and does not want to take any responsibility. In these cases is good to find experts, since every adversary is unique and it is not possible to prepare exactly the same scenario. For Incident handling are used prepared scenarios, which are modified to satisfy current event.

Competence of Manager must be technical, application, stress resistant with skill of control. Besides, he is responsible for removal of the mistakes which gives him huge authority. His target is to get out of unwanted and unpleasant status, when is under attack to known ground. During that move have to be sections of network categorized as well as incident itself. Incident can evolve and change, for example DDoS can hide Malware injection. Possible profile can be seen in Figure 4.13, where is seen wide knowledge, with small specialization in key services of organization.

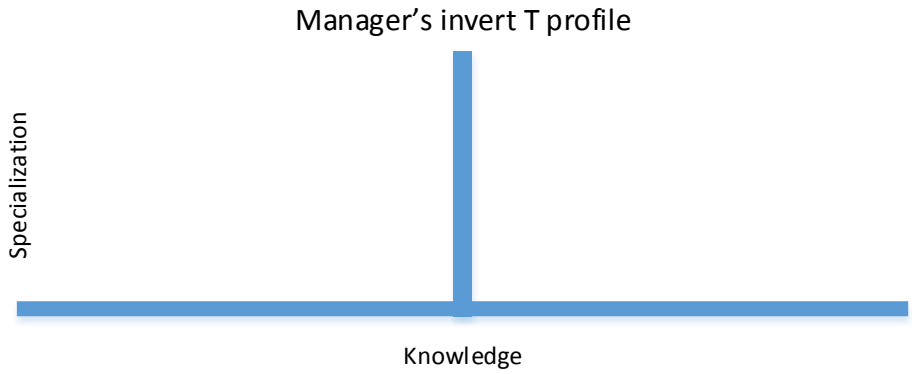


Figure 4.13 Knowledge vs Specialization "T" profile - Incident Manager

Categorization is important and is mostly done by value of assets or possible impact on company's repute. All this has to be done in collaboration with Top Management, since they are the highest authority in organization. Base for this evaluation is Risk analysis or in general Risk management. In addition Service level agreements play significant role and can have divested on whole organization. Incident manager should assure basic functionality of these services.

One example can be an attack on SCADA system running water Purifier. Manager has to decide if to turn off this system which is supplying 1500 households or be in risk of possible damaging or losing control over this system. Solution can be separation from Internet network and to use operators who are physically at location changing the flow of the water and controlling its quality.

In conclusion Incident manager is really stressful occupation and is not for everyone. Minimizing the impact needs decisive character and great knowledge of company run. In case of CII organization the Manager has to account for his act to Government and NSA.

5 Professional Development

So far it was discussed which competencies should have each role, however this gives only overview and does not specify ways how to get to it. For that is introduced following chapter with summary of offered certification and their brief categorization and are mentioned public and private universities offering Cyber security as their major. Besides, I am participating in creation of major Cyber security for high school in the Czech Republic, I know there is a problematic system of professional development and knowledge or skills are mostly gained from international certification Authorities.

5.1 International Certification Authorities

There are offered many certification regardless of areas and vendors, though most of them are covered by two big authorities – Pearson VUE [32] and Prometric [33]. I believe almost everyone has heard about Cisco Networking Academy. Their level system from CCENT to Architect with different specializations is tested through years and can be understood as an etalon of network certification. However for the need of this thesis it is necessary to see complex professional growth with focus on security roles mentioned in previous chapters. Following needs can be categorized as follows:

1. Audit/Risk Management – as was mentioned Risk management is important for Auditor as well as Manager or Architect, since it helps them to find financial support and to know weaknesses of their infrastructure. Some offered certification are CISA, CRISC, CGEIT, ISO, ITIL end many more, where each has different purpose and scope.
2. Forensic – this area is undisputedly important for every Asset administrator, Architect, CERT member or Incident Manager. It is important to know procedures how to monitor, collect data and analyse them. This is important for Post–Exploit, since in many cases happen, that the administrators do not even know someone infiltrated their systems. This certification helps to improve skill of paying attention to malicious behaviour within your infrastructure or system. Offered solutions are CHFI, CCFE, CCFP or CDFE.
3. Hack/Pen Test – these certification improves knowledge of your thinking, since for defending your network, it is necessary to think as your adversary, know their technics and more important test your network by Penetration testers. Penetration tests are really important and show skills and deeper understanding than can show automatized scan tool. These certification help you to know methodologies, types of attacks, usage of exploits to your favour, scripting and many more. However it goes in hand with price. Hack or Penetration tests certification can be categorized to:
    a. Application – significant focus on web application or software application, in general layer 7 of ISO/OSI model functionality. Certification are CSSLP, GWEB, OSWE or OSEE.
    b. Hack – in general large knowledge of whole ISO/OSI network model and possible attacks on each layer combined to infiltrate your infrastructure. Examples are OSWP, CEPT, CEH, LPT or CPT.
4. SCADA – one of the technical measures Manager and Architect has to cover are SCADA systems. These systems are specific for industry and are widely represented in CII, where are controlling power plants, water purifiers and many

more. This area is really specific and brings significant security risk. Offered solutions are CSSA, SANS or PCIP.

5. Network – network understanding is key knowledge base for Cyber security, since all the traffic, protocols, data are flowing through it, which brings most of the danger. Every security measure is based and situated within network and works with flows or packets. There is variety of network certification, regards to vendor, like Cisco, Juniper, Huawei and many more. Each vendor has specific technology, however basic principles are same for every network. Examples are CCNA to CCAr, HCNA to HCIE or JNCIA to JNCIE, every level has special Security branch and is up to the vendor how does it approach to it.
6. Operating System – in general are two or three main operation system branches; Linux, UNIX and Microsoft. Microsoft is mostly spread in households, however in Server solutions are mostly used systems based on Linux operation system and for some cases UNIX based systems, such as Sun, Solaris, BSD and others. Each system has different approach to work with policies, data and other things and because of that have different "default" security. Administrators and Architects should be aware of these diversities. Offered certification for each category are:
    a. UNIX – Oracle Certified Professional or Sun Certified System Administrator
    b. LINUX– LPI, RHCE or Linux +
    c. Microsoft – MTA, MCSA, MCSE or MCITP
7. Cloud, Storage, Virtualization – currently is a big issue to use mass storage for data which can be part of own infrastructure or can be outsourced even in a cloud. Nevertheless it does not have to be just data, but also virtualized servers, or in general resources for smooth run. In case of virtualization are moved images in real–time among locations, without notice and end user does not know where runs his system. This brings risks, since it is unknown what is happening with data, if are made backups and so on. For Cloud services are offered certification CCSK, IBM or from Amazon, in case of Storages are worthy to mention SNCP or EMSCA and for Virtualization are mostly introduced certificates from VMWare platform VCA, VCAP, RHCVA or CCP–V, in addition Cisco and others have own branch focused on Data Centres in general, where are all these technologies combined.
8. Information Security – previous parts are in common for Information engineer or Network engineer, however for the need of cyber security are specific areas, which are used for Security Engineer and ICT security overall knowledge. This knowledge is well described in CAP, SSCP, CISSP or CISM certification. These certification are well recognized and provide good study materials as well as differentiate different roles, similar to Cyber security law.

In conclusion is offered overview of possible certifications, however they are not mentioned all. As can be recognized, they are international, which brings problems with localization, local support, lectures, pricing and many more. Moreover, there are quality lectures offers made by local organizations, which are well localized. Example of it can be in the Czech Republic Alef Nula Inc., Network Security Monitoring Cluster and others with smaller or bigger number of lectors and made trainings. Moreover many vendors or business partners offer trainings of their technologies as a part in implementation.

There are other sources of knowledge on the Internet or in books, nevertheless one of the best is continuous development within company since certification are pricy, but are really good

source of information and even motivation. Many certification have to be regularly updated, since they have limited validity. This makes people work on them and keep on improvement, since any certification should not be taken for lifetime.

Suggested solution for each role or team can be as follows:

- Manager – should have gained certificates of the first, fifth, sixth and eighth category, since he needs to use Risk management and other processes well, know networking and platforms used within his system. This can be combined with for example CISSP Certification. For Manager in Czech is worthy to find training about local legislative acts. Based on his specialization can be taken any additional exams.
- Architect – in case of the architect are necessary all categories, since they are combining whole infrastructure. From this can be seen deep and wide knowledge base with specialization on specific technologies. However he needs to know the principles not completely details such as commands.
- Asset administrator – based on his specialization and administrated asset he should take certification training as well as training of networks, since it is really base and most of his devices do run on network.
- CERT – based on the offered services should be taken certificates. To satisfy basic services are partially necessary all categories.
- Incident Manager – his role is mostly to run and to minimize incident impact, for that are necessary categories one, four, five and eight. Furthermore he should know well company systems and regulations and suggest incident scenarios.

In conclusion, certification is a good way to become an expert, but has to be combined with practical experience on junior positions. This also helps to find the way of development, since each certification offers different scope and approach to problems.

5.2 Public schools

In previous chapter were introduced private certification authorities, which are in the most cases costly and many people cannot afford them, since if you have to fulfil requirements for potential job you already need to have this skill, though some employers are willing to invest to your education when they can see motivation. However best way for minimizing lack of security experts are schools or universities. So far there is no high school level of education focused on Cyber security, but this should be changed since year 2017/2018, when will be opened first pilot major. Next option are Bachelor, Master or MBA Cyber security majors. In Czech and even in Europe is not so strong emphasis on these majors and most programs are offered in the USA – for example at Carnegie Mellon University. After close analysis of Czech and offered Cyber security majors, it is found out that for Bachelor studies are few options. One of them is Brno University of Technology [34]. This is a regular major, however there are few majors with specialization on Cyber security, for example CTU Faculty of Information Technology, Faculty of Transportation Sciences and others. In case of Master studies, there are specialization at Masaryk University or at CTU Faculty of Electrical Engineering. So there is no specific major or follow–up Master for Bachelor students. Last option is a MBA program, which is offered by CEVRO Institute [35]. This program is for someone with previous experience and who wants to enhance his Manager specialization in Cyber security.

In sum, there is not so many options for students, they can choose some majors and try to take elective courses, however there are only two majors (both in Brno) fulfilling some of the competencies mentioned in previous chapters.

6 ISO 27k Family

The scope of this thesis is closely related to ISO 27k family, which covers run of ISMS, its implementation and many more. There is around 25 individual standards which give recommendations to run all parts of ISMS. During the thesis has been discussed the importance of Risk management for each role and its reflection to system improvement, audit or administration. It the following chapter will be discussed ISO 27005 closely from theoretical and practical point of view. Practical is based on work experience by telecommunication operator.

6.1 Information security risk management – ISO 27005

Risk management is a complex issue and it helps to analyse weak spots within your infrastructure and prepare countermeasures to improve it. The document serves to Manager, Architect, Auditor and Incident Manager and can be done in cooperation with CERT team based on their best practise.

The standard gives recommendation how to prepare own methodology and which specification it should have. There are several working methodologies such as CRAAM or COBIT, however these common methodologies have disadvantage it their specification. They are generally describing how to do risk analysis, nevertheless it might not cover some specific need of organization. ISO 27005 serves to organizations which want or must do own risk analysis, since it is giving these areas [7]:

- Scope definition – this includes general aspects such as borders of ISMS and more important approach to asset evaluation and possible impact in case of their unavailability. Some risks might not be taken into account, however if they are mentioned as a risk, the reasoning must be shown.
- Evaluation of Information security risk – covers recommendation how to identify risks, assets, threats, current measures, vulnerabilities and possible impact. Next part includes the risk analysis itself and mentions how to evaluate, either through Quantitative or Qualitative estimations and helps with assigning likelihood to each risk.
- Information security risk countermeasures – gives brief information how to handle the risks by their treating. The options for treating are reducing the possible risk (for example usage of HW, change configuration), accept the risk (possible impact is not significant and can be omitted) or evade the risk by not fulfilling the condition needed for risk. Last option is to share the risk with third parties (SLA).
- Monitoring – process of continuous evaluation of risk analysis, since infrastructure is changing every day, by using new systems, programs, hardware and with it possible assets and vulnerabilities.
- Risk consulting – in case the risk management is done by the organization it is recommended to invite auditors for regular checks, if own methodology is designed well and fulfils all requirements.

From the points above can be seen that Risk management is a process and can be described by PDCA, as is shown in Figure 6.14.

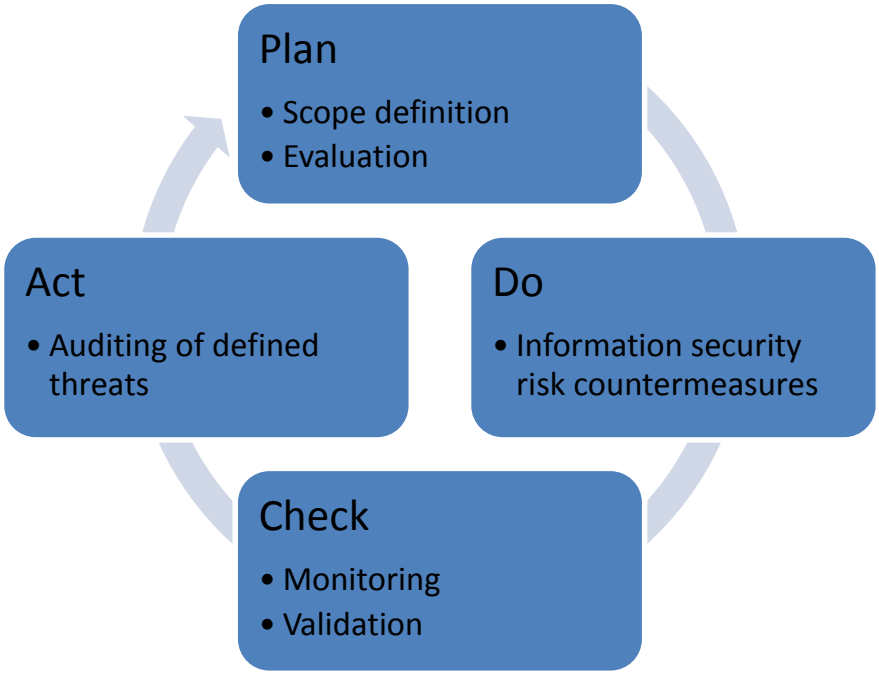


Figure 6.14 PDCA - Risk management

Creating of own methodology has many advantages, since you as an owner of the infrastructure know about it the most. You can give the best input data to the risk analysis, define key systems and suggest best countermeasures. The methodology is tailor–made to the needs of organization. It is important to realize Risk management is not a one–time action, it has to be continuously updated and filled with current data from database and to follow strategy of company.

6.2 Risk analysis – Telecommunication operator

In previous chapter is discussed what covers and recommends risk analysis how it should be done. However the biggest question which is faced is how to seize infrastructure of Telecommunication operator, where are thousands base stations (BTS), Remote Subscriber Units (RSU), HOSTs, hundreds of buildings and servers, many different technologies and this whole is spread around whole Czech Republic.

The project of creation tailor–made Risk Management is not matter of months but years. Regards to PDCA cycle, the step of planning takes long time, since if you do not prepare your model well, it is necessary to start again. However it does not mean next steps are not made, just they are carefully validated.

Telecommunication operators are big companies, since they change their owners, create, own infrastructure and invest big money to technology. This brings many problems, since many critical systems or services had to be differentiate. From historical point of view it is not easy, since when company is investing into improvement it does not count with future changes of an owner. During procedure were several questions discussed:

- What is the scope of Risk Management? The scope is really wide, some services for monitoring infrastructure are covering whole Czech Republic, but Risk analysis has to include them. Next problem is how to get information about them, since there are hundreds of Asset administrator and Risk analysis of ISMS includes threats

from Physical security to Application security. There can be approach through validation of assets or services.

- How to get valid data? Since company is in a big change, the data might not be valid, since what is at the time of answering questions problem might be in next month solved. Next problem is boundary of network. Even though severity of Risk analysis during false information may be given, since labours are busy with own work. It has to be counted with likelihood of validity and check data from different sources as was mentioned for asset evaluation. Next issue is almost zero possibility of validation, since physical control of remote buildings and its configuration would require enormous resources.

- Is our model covering all the aspects? As was mentioned, infrastructure is developing and it is difficult to create whole model counting all the issues. As a result our model is flexible, specific and robust. Flexible in matter of updating the input data databases, which evaluate the final Risk, specific in the focus on the company boundaries and robust for future enhancement.

As can be seen, theoretical and practical experience may differ and brings many issues, which have to be solved, since for Audit all the required criteria have to included, otherwise it can bring possible failure.

7 Conclusion

Main target of this thesis is to define impact of Cyber security law and regulations related to it in area of the Czech Republic. It was done by analysis of job offers, ISO/IEC 27000 family, work experience and identification of national or international certification programs for a specified role of Manager, Architect, Auditor and Asset Administrator, who are mentioned in paragraph 5 of law 181/2014 Coll. and for CERT teams, which play key role in handling of massive incidents on National, Government or international level. Last role is an Incident Manager which is mentioned in Incident management of ITIL.

Based on these information and gained experience are suggested competencies for each role. This brings totally new view to this issue, since the only requirements mentioned in the law are three year work of experience on related position. During gathering the information it was a big issue to create overall knowledge, since this topic is really wide, was not discussed during studies and is completely new on Czech market. Fortunately due to work experience it was possible to analyse information and suggest competence models, which are the core of this thesis. These models cover which skills and knowledge are important for specified roles. These called "topologies" are defining scope of work for each role as well as describe comparison between knowledge and specialization to specific area. This approach brings new view and enables to see profile in entire perspective. The searches show, that there is not unified system of education of these roles. This can be justified by the short efficiency of the law in the Czech Republic, however Czech is one few countries around the world having own law. Though before are discussed regulations and the law, is presented the motivation for Cyber security and what brings the future. Following chapter focuses on acts preceded the law creation, which continuously moves to closer overview of law and regulations.

Practical part is covering the roles and Risk management. First role is an Auditor, who has as it was shown the best system of education, which can be certified by many organization, with good model of professional development. The knowledge base of the Auditor is based on ISO/IEC 27000 family, where is described how to approach to ISMS. Most of audits are focused on satisfying ISO 27001 and to check in detail Risk analysis, which requirements are described in ISO 27005. On the other hand for the Architect it does not exist any specific professional tree, since their scope is based on technologies, which can wary from organization to organization and more important become obsolete soon. As a result was decided to mention competencies covering security elements to satisfy technical measures, which has to be taken into account when topology is created and administrated. However technical measures would be misused if is not done good analysis by Manager and are not prepared organizational measures and processes to make labours respect them. Manager has to collaborate on this with the Architect, however his specialization is to organize, nevertheless he should have technical background, which will be helpful in assert of security policies, organizational changes, defining direction of system security and last but not least asking for budget at Top Management. This task is the most difficult, since security department is costly, even though it does not generate any income to the organization until company has to face an incident. Significant part of security costs are support services and resources for maintenance of security elements.

Further mentioned is the Incident manager, who helps the organization to minimize the impact during the incident by having enormous responsibility and knowledge about the infrastructure. Next and last role is the Asset Administrator, who cares about own asset and network on which it is running. This task is mostly technical and should have narrow specialization in his area of work. Last mentioned are CERT teams. In our region are key CERTs – GOVCERT (Government CERT, which is part of NCKB) and CZ.NIC (which is

National CERT and signed Memorandum of Collaboration with NSA). Work of CERT is to gather incidents from respective organizations and to give recommendation how to solve them. GOVCERT is working with CII and SIS and can invite experts from outside to help solve their problems, on the other hand CZ.NIC collaborates with other private CERTs and creates database open to public. Moreover, it has other activities where one of them is to increase public awareness of Cyber security or Information security. These two CERTs have defined a scope of work in the law and the Memorandum, however private CERTs are working on three or four key pylons, which help to improve their reputation. Key organization covering worldwide CERTs is Trusted Introducer (Europe region) and FIRST (Worldwide).

Next chapter is covering professional development, after defining competencies and role models, it has to be defined where to get required knowledge. This is problematic, since there is variety of Certification, however public or private schools offer just few options. This should be changed especially because of huge job market demand on qualified professionals, who are able to be cover positions of CII and SIS mentioned in the Cyber security law. There is a need of other experts who are able to monitor traffic, implement solutions and handle incidents and others.

Last mentioned is Risk analysis, which is closely described in ISO 27005. This document is a base for Risk Management and serves as a significant document to all mentioned roles. Based on this document it is created improvement strategy of system, shortcomings are found within own infrastructure, which have to be taken into account and moved to acceptable threat. Significant documents coming with Risk management are Statement of Applicability, Business Impact Analysis and methodology used for evaluation of risks and assets.

Thanks to new areas creating new social revolution, it will be increased a demand of Security experts, who are even now in huge lack. However this issue is not just about learning theoretical and enhancement of practical knowledge, but should go in hand with life attitude and can be understood as a life philosophy. This thesis can be taken as a base for future improvement, which may be in specification of role learning plans and study materials creation for specific domain. Since the Architect is the most technical field and many areas are already taught, the best for needs of the CTU FEE would be to create a new major focused on Cyber security for the Architect.

8 References

[1] Nařízení vlády, kterým se mění nařízení vlády č. 432/2010 Sb., o kritériích pro určení prvku kritické infrastruktury. In: *Sbírka zákonů*. Praha: Tiskárna Ministerstva vnitra, 2014, ročník 2014, částka 127, číslo 315.

[2] Vyhláška o bezpečnostních opatřeních, kybernetických bezpečnostních incidentech, reaktivních opatřeních a o stanovení náležitostí podání v oblasti kybernetické bezpečnosti (vyhláška o kybernetické bezpečnosti). In: *Sbírka zákonů*. Praha: Tiskárna Ministerstva vnitra, 2014, ročník 2014, částka 127, číslo 316.

[3] Vyhláška o významných informačních systémech a jejich určujících kritériích. In: *Sbírka zákonů*. Praha: Tiskárna Ministerstva vnitra, 2014, ročník 2014, částka 127, číslo 317.

[4] MAISNER, Martin. *Zákon o kybernetické bezpečnosti: komentář*. Vydání první. Praha: Wolters Kluwer, 2015. Komentáře (Wolters Kluwer ČR). ISBN 978–80–7478–817–8.

[5] *Směrnice pro auditování systémů managementu*. 2. Praha: Úřad pro technickou normalizaci, metrologii a státní zkušebnictví, 2012.

[6] *Směrnice pro audit systémů řízení bezpečnosti informací*. 1. Praha: Úřad pro technickou normalizaci, metrologii a státní zkušebnictví, 2013.

[7] *Řízení rizik bezpečnosti informací*. 2. Praha: Úřad pro technickou normalizaci, metrologii a státní zkušebnictví, 2013.

[8] *Systémy řízení bezpečnosti informací – přehled a slovník*. 3. Praha: Úřad pro technickou normalizaci, metrologii a státní zkušebnictví, 2014.

[9] *Systémy řízení bezpečnosti informací – Požadavky*. 2. Praha: Úřad pro technickou normalizaci, metrologii a státní zkušebnictví, 2014.

[10] *Soubor postupů pro opatření bezpečnosti informací*. 2. Praha: Úřad pro technickou normalizaci, metrologii a státní zkušebnictví, 2014.

[11] *Směrnice pro implementaci systému řízení bezpečnosti informací*. 1. Praha: Úřad pro technickou normalizaci, metrologii a státní zkušebnictví, 2011.

[12] *Požadavky na orgány provádějící audit a certifikaci systémů řízení bezpečnosti informací*. 1. Praha: Úřad pro technickou normalizaci, metrologii a státní zkušebnictví, 2008.

[13] Processes: Overview of TI Processes. *TF–CSIRT Trusted Introducer* [online]. Hamburg: PRESECURE, 2013 [cit. 2016–04–30]. Dostupné z: https://www.trusted–introducer.org/processes/overview.html

[14] *Guidelines for information and communication technology readiness for business continuity*. 1. Switzerland: ISO Copyright office, 2011.

[15] *Business continuity management systems – Requirements*. 1. Switzerland: ISO Copyright office, 2012

[16] CSIRT Services. *CERT* [online]. Carnegie Mellon University: Pittsburgh, PA 15213–2612, 2016 [cit. 2016–04–30]. Dostupné z: http://www.cert.org/incident–management/services.cfm

[17] IRCA Certified Training. *IRCA* [online]. London: 10 Furnival Street, 2016 [cit. 2016–04–30]. Dostupné z: http://www.irca.org/en–gb/Training/IRCA–Certified–Training/

[18] KNAPP, Eric. *Industrial network security: securing critical infrastructure networks for Smart Grid, SCADA , and other industrial control systems*. Waltham, MA: Syngress, c2011. ISBN 15–974–9645–6.

[19] AMOROSO, Edward G. a John R. VACCA. *Cyber attacks: protecting national infrastructure*. Student ed. Waltham, MA: Butterworth–Heinemann, 2013. ISBN 978–012–3918–550.

[20] WINKLER, J. R. a John R. VACCA. *Securing the cloud: cloud computer security techniques and tactics*. Student ed. Waltham, MA: Syngress/Elsevier, 2011. ISBN 978–159–7495–929.

[21] Certifikace CISA. ICASA Serving IT Governance Specialist, Czech Republic Chapter [online]. Praha: ISACA Czech Republic Chapter, 2008 [cit. 2016–05–01]. Dostupné z: http://www.isaca.cz/cs/certifikace–cisa

[22] BEHROUZ A. FOROUZAN., J. R. a John R. VACCA. *Data communications and networking: cloud computer security techniques and tactics*. Fifth edition. New York: McGraw–Hill, 2013, 290 p. ISBN 978–007–1315–869.

[23] FIRST Improving Security Together [online]. Morrisville: FIRST.org, 1995 [cit. 2016–05–09]. Dostupné z: www.first.org

[24] BMC. *ITIL Incident Management: Best Practices & Process Flow –BMC* [online]. Houston: BMC, 2014 [cit. 2016–05–09]. Dostupné z: www.bmc.com

[25] *Systémy managementu kontinuity podnikání – Požadavky*. 2. Praha: Úřad pro technickou normalizaci, metrologii a státní zkušebnictví, 2013.

[26] *Systémy managementu kontinuity podnikání – Pokyny*. 1. Praha: Úřad pro technickou normalizaci, metrologii a státní zkušebnictví, 2015.

[27] *CZ.NIC* [online]. Praha: CZ.NIC, 2016 [cit. 2016–05–11]. Dostupné z: www.nic.cz/

[28] *Národní centrum kybernetické bezpečnosti* [online]. Praha: NBÚ, 2016 [cit. 2016–05–11]. Dostupné z: www.govcert.cz/cs/

[29] *Národní bezpečností úřad* [online]. Praha: NBÚ, 2016 [cit. 2016–05–11]. Dostupné z: www.nbu.cz/cs/

[30] *PCI Security Standards Council* [online]. Wakefield: PCI Security Standards Council, LLC, 2006 [cit. 2016–05–18]. Dostupné z: www.pcisecuritystandards.org

[31] *(ISC)²* [online]. Clearwater, Florida: (ISC)2, Inc., 1996 [cit. 2016–05–18]. Dostupné z: www.isc2.org

[32] *Pearson Vue* [online]. Bloomington, Minnesota: Pearson Education Inc, 1996 [cit. 2016–05–18]. Dostupné z: www.pearsonvue.com

[33] *Prometric* [online]. Baltimore: Prometric Inc., 2016 [cit. 2016–05–18]. Dostupné z: www.prometric.com

[34] Detail oboru Informační bezpečnost. *Vysoké učení technické Brno* [online]. Brno: VUT Brno, 2016 [cit. 2016–05–20]. Dostupné z: www.vutbr.cz/studium/ects–katalog/detail–oboru?oid=10687

[35] MBA – Management a kybernetická bezpečnost. *CEVRO Institut* [online]. Praha: CEVRO Institut, z.ú., 2015 [cit. 2016–05–20]. Dostupné z: www.cevroinstitut.cz/cs/clanek/mba–management–a–kyberneticka–bezpecnost/

9 Table of Figures

Figure 4.1 Relation among Private&Public CERT 19
Figure 4.2 CERT Services 21
Figure 4.3 Manager's "topology“ 23
Figure 4.4 PDCA - Manager 25
Figure 4.5 Knowledge vs Specialization “T” profile - Manager 25
Figure 4.6 Knowledge vs Specialization “T” profile - Architect 26
Figure 4.7 Architect's topology 28
Figure 4.8 Auditor's approach 31
Figure 4.9 Knowledge vs Specialization “T” profile - Auditor 32
Figure 4.10 PDCA – Auditor 33
Figure 4.11 Knowledge vs Specialization “T” profile - Administrator 34
Figure 4.12 Asset Admin problem scope 35
Figure 4.13 Knowledge vs Specialization “T” profile - Incident Manager 36
Figure 6.14 PDCA - Risk management 41

10 Vocabulary & List of Shortcuts

- Due diligence – pojem označující plnění závazků vůči naším mezinárodním partnerům a smlouvám s nimi, kybernetická bezpečnost se neřeší pouze na státní, ale i na mezinárodní úrovni.
- Status of Cybernetic danger – stav kybernetického nebezpečí, který může vyhlásit předseda Národního bezpečnostního úřadu v případě, že je ohrožena bezpečnost informací nebo informačních systémů.
- Self–determination – každá osoba má právo na informační sebeurčení.
- CII – Critical Information Infrastructure – Kritická informační infrastruktura
- SIS – Significant Information System – Významný informační systém
- CERT – Computer Emergency Response Team
- CSIRT – Computer Security Incident Response Team
- NSA – National Security Agency – Národní bezpečností úřad (NBÚ)
- NCSC – National Cyber security Centre – Národní centrum kybernetické bezpečnosti, také lze označit za vládní CERT.
- HA – High Availability – Vysoká dostupnost, redundancí dochází k zajištění dostupnosti.
- CISA – Certified Information Systems Auditor
- ISACA – Information Systems Audit and Control Association
- PDCA – Plan–Do–Check–Act
- SCADA – supervisory control and data acquisition
- ISO – International Standardization Organization
- IRCA – International Register of Certificated Auditors
- ITIL – Information Technology Infrastructure Library
- IS – Information System
- CIA – Confidentiality, Integrity and Availability
- CIA – Central Intelligence Agency
- FIRST – Forum of Incident Response and Security Teams
- ENISA – European Network and Information Security Agency
- AFCEA Armed Forces Communications and Electronics Association
- ITU – International Telecommunication Union
- ISACA – Information systems Audit and Control Association
- SoA – Statement of Applicability
- BIA – Business Impact Analysis
- CCENT – Cisco Certified Entry Networking Technician
- CRISC – Certified in Risk and Information Systems Control
- CGEIT– Certified in the Governance of Enterprise IT
- CHFI – Computer Hacking Forensic Investigator

- CCFE – Certified Computer Forensics Examiner
- CCFP – Certified Computer Forensics Professional
- CDFE – Certified Digital Forensics Examiner
- CSSLP – Certified secure software lifecycle professional
- GIAC – Global Information Assurance Certification
- GWEB – GIAC Web Application Defenders certification
- OSWE – Offensive Security Web Expert
- OSEE – Offensive Security Exploitation Expert Certification
- OSWP – Offensive Security Wireless Professional
- CEPT – Certified Expert Penetration Testers
- CEH – Certified Ethical Hacking
- LPT – Licenced Penetration Tester
- CPT – Certified Penetration Tester
- CSSA – Certified SCADA Security Architect
- SANS – Escal Institute of Advanced Technologies
- PCIP – Payment Card Industry Professional
- CCNA – Cisco Certified Network Associate
- LPI – Linux Professional Institute
- RHCE – Red Hat Certified Engineer
- MTA – Microsoft Technology Associate
- MCSA – Microsoft Certified Solutions Associate
- MCSE – Microsoft Certified Solutions Expert
- MCITP – Microsoft Certified IT Professional
- CCSK – Certificate of Cloud Security Knowledge
- SNCP – Storage Networking Certification Program
- EMCSA – EMC Storage Administrator Certification
- VCA – VMWare Certified Associate
- VCAP – VMWare Certified Advanced Professional
- RHCVA – Red Hat Certified System Administrator
- CCP-V – Citrix Certified Professional – Virtualization
- CAP – Certified Authorization Professional
- SSCP – Systems Security Certified Practitioner
- CISSP – Certified Information Systems Security Professional
- CISM – Certified Information Security Manager