View metadata, citation and similar papers at core.ac.uk

brought to you by CORE

provided by Repository of the Academy's Library

HADMÉRNÖK

IX. Évfolyam 1. szám - 2014. március

Krasznay Csaba – Török Szilárd
krasznay.csaba@uni-nke.hu – torok.szilard@gmail.com

HUNGARY'S CYBER DEFENSE READINESS FROM THE PERSPECTIVE OF INTERNATIONAL RECOMMENDATIONS

Abstract

A country's cyber defense structure is usually very complex and needs interagency cooperation. All countries have a different governance structure, but usually the ministries responsible for internal and external defense have an important role. This is confirmed by recommendations from various international organizations that show best practices for the creation of national cyber defense strategies. The goal of this study is to overview the structure of Hungarian cyber defense and its compliance with international recommendations.

Egy ország kibervédelmi szerkezete általában meglehetősen összetett, ezért elengedhetetlen az egyes elemek közötti együttműködés. Az országok eltérő kormányzati szerkezettel bírnak, azonban általános a minisztériumok felelősége a belső- és külső védelmi feladatok ellátásában. Számos nemzetközi szervezet, mint "legjobban bevált gyakorlat"-ként ajánlja a nemzeti kibervédelmi stratégia létrehozását. Ezen publikáció fő célja, hogy bemutasa a Magyarország kiber védelmi struktúráját, illetve összevesse azt a nemzetközi ajánlásokkal.

Keywords: *cyber defense, international recommendations, strategies ~ kibervédelem, nemzetközi ajánlások, stratégiák*

INTRODUCTION

As information technology growing quickly and broadly, the vulnerabilities of technology are exploited to a higher extent. With the in-depth knowledge and usage of IT it is more optimal and cost efficient to manage the inevitable data and information acquisition processes in various fields of intelligence, crimes and military warfare.

IT crimes (or cyber-crimes) need to be distinguished according to information technology users and their motivation: these can be amongst others mainly hackers (white or black hat – they mostly driven by financial interests), industrial spies, external and internal experts, and IT criminals.

To lay down a country's cyber defense tasks need the cooperation of various military, national defense and civil organizations. There are various different international recommendations that help in developing of a national cyber defense strategy and legislation system, and creating of roles and responsibilities. Although the defense structure is different country by country, some organizations have a special role in this hierarchy.

In Hungary, the Act L. of 2013 on the electronic information security of state and municipal organization and Hungary's National Cybersecurity Strategy deal with the cyber defense structure. The whole legislation system is constantly evolving, but its current state is suitable to take a snapshot and analyze its compatibility with international recommendations.

Based on the above it is necessary and relevant to design and develop a cyber defense center in Hungary, namely a Cyber Security Centre. The government built up a centralized IT operation and development company in the past few years called NISZ Zrt. (National Info Communication Service Provider and its subsidiaries) which has a central role. The operation of the National Telecommunication Core Network's (NTG) network security is being operated by the NISZ as of summer of 2013 – in close cooperation with the newly established Government Incident Response Team (Gov-CERT – Hungary).

This study uses the following guidance sets as a base point: ITU's National Cybersecurity Strategy Guide, ENISA's National Cyber Security Strategies and NATO's Cooperative Cyber Defence Centre of Excellence (CCD CoE) National Cyber Security Framework Manual and derives their requirements to the Hungarian situation.

INTERNATIONAL RECOMMENDATIONS

International Telecommunication Union (ITU)

ITU published its recommendations in 2011 under the title of National Cybersecurity Strategy Guide. This guidance was one of the first in this topic and its aim is to help settling down a national cyber security system. This publication recommends 10 steps as important strategic goals.

1. Top Government Cybersecurity Accountability: Top government leaders are accountable for devising a national strategy and fostering local, national and global cross-sector cooperation.
2. National Cybersecurity Coordinator: An office or individual oversees cybersecurity activities across the country.
3. National Cybersecurity Focal Point: A multi-agency body serves as a focal point for all activities dealing with the protection of a nation's cyberspace against all types of cyber threats.
4. Legal Measures: Typically, a country reviews and, if necessary, drafts new criminal law, procedures, and policy to deter, respond to and prosecute cybercrime.

5. National Cybersecurity Framework: Countries typically adopt a Framework that defines minimum or mandatory security requirements on issues such as risk management and compliance.
6. Computer Incident Response Team (CIRT): A strategy-led program contains incident management capabilities with national responsibility. The role analyses cyber threat trends, coordinates response and disseminates information to all relevant stakeholders.
7. Cybersecurity Awareness and Education: A national program should exist to raise awareness about cyber threats.
8. Public-Private Sector Cybersecurity partnership: Governments should form meaningful partnership with the private sector.
9. Cybersecurity Skills and Training Program: A program should help train cybersecurity professionals.
10. International Cooperation: Global cooperation is vital due to the transnational nature of cyber threats.

This recommendation designates those responsible governmental and civil players who have some role in the execution of strategic tasks. The key players are the followings:

- The Government, in Hungary the Prime Minister's Office
- The Parliament
- Owners and operators of critical infrastructures
- Courts
- Law enforcement authorities
- Intelligence organizations
- Manufacturers of IT security products
- Academies
- International partners
- Citizens

In Hungary strategic decisions are made by the Prime Minister's Office. The Ministry of Public Administration and Justice is responsible for the legislation and supervises the National Security Authority and is also one of the sustainers of National University of Public Service (NUPS). The Ministry of Interior supervises the critical infrastructures (through the National Directorate General for Disaster Management), the law enforcement authorities (Police, Counterterrorism Center), some intelligence organizations (Constitution Protection Office, Special Service for National Security with the Gov-CERT inside) and partially the National University of Public Service. The Ministry of National Development is responsible for the development of National Cybersecurity Framework. All of the aforementioned organizations are involved in international cooperation. ITU's enumeration does not deal with the military perspective.

European Network and Information Security Agency (ENISA)

ENISA is the European Union's cybersecurity agency which published its National Cyber Security Strategies – Practical Guide on Development and Execution book in December 2012. It proposes 20 steps for the development of a national cybersecurity strategy.

1. Set the vision, scope, objectives and priorities.
2. Follow a national risk assessment approach.
3. Take stock of existing policies, regulations and capabilities.
4. Develop a clear governance structure.
5. Identify and engage stakeholders.
6. Establish trusted information-sharing mechanisms.
7. Develop cyber-security contingency plans.
8. Organize cyber-security exercises.

9. Establish baseline security requirements.
10. Establish incident-reporting mechanisms.
11. Make citizens aware.
12. Foster R&D.
13. Strengthen training and educational programs.
14. Establish an incident response capability.
15. Address cybercrime.
16. Engage in international cooperation.
17. Establish a public–private partnership.
18. Balance security with privacy.
19. Evaluate.
20. Adjust the national cyber security strategy.

This guidance does not specify any organizations, but key players can be easily identified from the examples and use cases. It strengthen the roles of those organizations that can be derived from ITU's guidance.

Hungarian legal background

In 2013 the Hungarian government defined the National Cyber Security Strategy of Hungary (Government decree [2] of 1139/2013. III.21.) and based on this decree the act about „Electronic information security of state and local government institutions" [3] (hereinafter abbreviated as: IBTV) was ratified.

There are many previous regulations on the security of domestic systems, government institutions and networks related to public administration. The government's intention was to manage this field by creating detailed measures such as:

- Act C. of 2003 about Electronic Telecommunication.
- The related IHM decree of 27/2004. (X. 6.) (about the establishment, operation, competence of the duty system of the postal branch and the IT and electronic telecommunication branch, furthermore about the notification and liaising obligations of the designated service providers, the actions related to the network security of these service providers.
- Government decree of 100/2004. (IV. 27.) about the emergency management and classified period operation system in electronic telecommunication, about the tasks of public administration organizations, and the provisions of proper conditions for their operation.
- The NMHH decree of 4/2012. (I. 24.) about data protection and confidentiality obligations related to public electronic telecommunication service, special terms of data management and confidentiality, the security and integrity of networks and services, the management of traffic and invoice figures, furthermore the regulations related to ID display and call forwarding.

As part of the Digital Renewal Action Plan (2010-2014) it became necessary to create a legal background that is better suited to the development of domestic systems and the circumstances of electronic public administration.

Accordingly in spring 2012 the government decree of 83/2012. (IV. 21.) was adopted about the regulated electronic administration services and about the services to be mandatorily provided by the government, the government decree of 84/2012. (IV. 21.) about the designation of institutions related to electronic administration, furthermore the government decree of 85/2012. (IV. 21.) about the detailed rules and regulations of electronic administration. It is important to mention that these government decrees determine the minimum requirements towards service providers concerning the secure operation of the services.

The definition background of regulated electronic administration services is determined by the Act of 2004. CXL, Article 172 (hereinafter referred to as: 'Ket.' about the general rules of public administration procedures and services. The primary goal of the act is to establish those new legal institutions which provide procedure and data management guarantees to citizens and businesses, and makes it possible for them the usage of electronic communication, and eliminate over-regulations.

It has to be emphasized that data forwarding processed through the NTG network has to comply with the requirements of personal data protection which is elaborated in the act of 2003 C. Article 155, furthermore - with proper technological and logistics measures – it is necessary to hinder the interception, storage or surveillance of forwarded communication or data traffic related to the communication, moreover to hinder unauthorized or accidental access to data traffic related to communication.

The Cyber Security Centre in Hungary

Based on the above goals, expectations and regulations, a need for the establishment of a Cyber Security Centre (CSC) has arisen within the governmental IT operation structure. Due to the operational and organizational capabilities of a central IT operation, the NISZ is considered to be the most competent entity for the implementation.

The Cyber Security Centre needs to be scalable, adjustable to the defense requirements of organizations and their information systems, furthermore it needs to continuously provide information to the NISZ and its governmental clients. A centrally monitored and managed cyber security contributes to the reduction in cyber security risks and threats and it could even turn into a proactive defense system.

As an important part of the planning procedure it is necessary to list those types of solutions which can tackle the current cyber security challenges.

1. Monitoring center and incident management
2. (log analysis)
3. Network security analysis and malware laboratory
4. Defense capability against data leakage

The Cyber Security Centre receives input data from the National Telecommunication Core Network (NTG) namely the log files of devices that provide the IT security functions for NTG, moreover receives the network security information collected by GovCERT from external sources.

Based on the processing of input data the present relations and correlations, vulnerabilities and risks are defined, and based on this, real time or preventive warnings need to be forwarded to the operators and governmental users.

The Cyber Security Centre needs to meet some general requirements such as:

- Needs to provide an efficient solution for the analysis of the network's data traffic
- Needs to be available continuously in order to centrally process and evaluate the received log files in a reliable manner.
- Needs to detect and manage intruder suspect events and targeted attacks efficiently
- Needs to implement efficient and competent incident management supported by more comprehensive reports.

The detailed content of the listed items

1. Monitoring Centre, Incident Management: The expenditure on defense and other security measures will be efficient in case the CSC is able to interpret the signals of increased security incidents and events and to efficiently interfere, furthermore to maintain an intense technical and professional cooperation with competent authorities regarding specific cases.

Increasing reporting and detecting capability

a) The detection and more efficient reporting on increased security events (due to developments) are of key significance. Accordingly, NISZ being responsible for IT operation is expected to employ IT security professionals with relevant qualifications and experience, furthermore it is expected to produce sufficient early and trend reports for all professional and management levels.

b) In order to reach this, log processing needs to be developed according to the expectations of modern cyber defense.

2. IT security log analysis

   a) In order to collect and redundantly store log files, the extension of log collector systems is needed.

   b) Also the extension the analysis of log files is necessary (quantity, quality, etc.), including a more efficient processing and evaluation – e.g.: the log files of different services and applications need to be adjusted to the same level.

   c) It is necessary to track the samples from – even subsequently solved - incidents to processing systems. This requires the introduction of a framework system that makes it possible to be easily conducted by a monitoring employee without developer expertise.

   d) It is necessary to integrate the heterogenic log analysis in the IT operation systems and the log registration infrastructures into one frame system (with the introduction of proper methodology and professional solution).

3. Network traffic analysis

   a) The online analysis of the traffic is crucial to improve security therefore the most suitable product needs to be integrated into the system.

   b) The network analytical device should be able to monitor, interpret the total network traffic, and trace back immediately any communication between two endpoints. The visualization layer enables online processing, and a potential intruder attempt can be detected.

   c) The solution needs to be able to save the total monitored traffic, and complement the saved traffic with further information necessary for interpretation.

   d) The potential damages can be determined from the saved data and can be used later as evidence.

   e) The generated reports, warnings and trends need to be connected to the incident management, log analysis and report generating subsystems.

   f)

4. Data Loss Prevention solutions: Based on the current user, end point and mobile device structure and user habits within IKK two types of solutions need to be developed against data leakage Endpoint and network Data Loss Prevention (DLP and Net-DLP)

   a) These solutions ensure the tracking and control of inward and outward data traffic at endpoints, and ensure the collection of evidence.

   b) Mobile Device Management (MDM)

   c) Smart phones and tablets are quite popular in the government all these devices carry potential data leakage risks due to their storage capacity and mobile data medium functions (USB key, SD card, etc.).

   d) Their usage is manually untraceable, it is necessary to define client level and within that user profiles, and manage the related software packages and rules.

5. Ensuring data protection and legal compliance
   a) The NISZ as the central telecommunication and IT service provider of the government, is in a position facilitate adherence to electronic information security and data protection rules on an operational level at the institutions where its services are provided.
   b) Therefore the preparation of a central network and information security service level agreement (Security SLA) is necessary. This document lays down those fundamental technical measures that guarantee cyber security on an operational level.
   c) The technical measures listed in the Security SLA need to be applied to governmental clients individually and according to the specifications of governmental institutions served by NISZ. Based on this, the specific technical measures of the individual service agreement need to be correlated to the related electronic information protection and data protection rules.

ACHIEVABLE CYBER SECURITY RESULTS

This study examines the proper cyber security practice through international and domestic expectations and legal backgrounds overviewed in the study, and through the well-known public cyber security threats.

The goal of the aforementioned described Cyber Security Centre is to create a system to support governmental endpoint and network security protection, which enables to reveal threatening events and risks, control and management of necessary measures, furthermore ensures the continuity of confidentiality, integrity and availability. The target groups of the Centre are the National Telecommunication Core Network (NTG) and joining institutions.

The Cyber Security Centre needs to be scalable, adjustable to the defense requirements of organizations and their information systems, furthermore it needs to continuously provide information to the organizations, and meanwhile it needs to be a centrally controllable and manageable endpoint and network security system.

References

[1] Act L of 2013 about the electronic information security of state and municipal organizations

[2] Government decree about Hungary’s National Cyber Security Strategy

[3] Wamala, F.: *The ITU National Cybersecurity Strategy Guide.* International Telecommunication Union, 2011.

[4] *National Cyber Security Strategies – Setting the course for national efforts to strengthen security in cyberspace*. European Network and Information Security Agency (ENISA), 2012.

[5] Klimburg, A. (ed): *National Cyber Security Framework Manual*. NATO CCD COE Publication, Tallinn 2012

[6] Act XLIII. of 2010 about central public administration organizations, and members of the government and secretaries

[7] 233/2013. (VI. 30.) government decree about the competence and authority of the incident management center of facilities and essential facilities, branch incident management centers, and governmental incident management centers of electronic information systems.

[8] 36/2013. (VII. 17.) Ministry of Justice decree about the branch rules regarding the monitoring and control of closed end electronic information system security.

[9] Act CLXVI of 2012 about the identification, appointment and protection of essential systems and facilities.