Magyar Rendészet 2016/3. 155–171.

Areas for Police Information Network Information Security Development

FEHÉR Judit[1]

This information security assessment provides an objective and at the same time comprehensive picture of the state of security, control and risk management areas. To determine the information security context and to obtain real values, an examination of the documents and information systems which are part of the network, as well as potential threats and dangers to the network, must be carried out. In accordance with Hungarian Law, the Hungarian Police must guarantee the security of police information networks, therefore, development must focus on the administrative, logical and physical areas. These areas are determined at an organisational level and at the level of police information networks. The tasks and measures necessary to achieve security strategy objectives and to fulfil requirements are outlined in relation to these areas.

Keywords: *information security, security class, strategy, measures, administrative, physical, logical*

In order to determine information security tasks for the police information systems, and especially the security of its information networks, an analysis concentrating on several areas over a long span of time must be conducted. The primary starting point is the current status quo. Police information networks will be analysed in the context of police information systems.

When examining the information security of systems, from an administration security point of view, document analyses must be carried out, where the security status of each police information system is determined by sampling, which can be then extrapolated to the system as a whole. In order to obtain real values, during the sampling process the potential threats and dangers to priority information networks must be examined, for which document analyses on the administrative area must be carried out, and vulnerability inspections and risk analysis must be conducted on the physical area. These results raise real practice-oriented information security questions, based on which any deficiencies and experiences of the requirements for priority police information networks can be determined. The purpose would be to make them comply with the required security level and protection on a system level. However, the current analysis is limited to the administrative context, and only reveals the results of infor-

1 FEHÉR Judit police lt. col. Deputy State Secretary for IT Department for Informatics Division for Information Technology and Defense, PhD student, Obuda University, Security Doctoral School
Judit FEHÉR r. alezredes, főosztályvezető-helyettes, Informatikai Helyettes Államtitkárság, Informatikai Főosztály, Információtechnológiai és Védelmi Osztály, PhD-hallgató, Óbudai Egyetem, Biztonságtudományi Doktori Iskola
feherjenator@gmail.com

mation security document analyses. The whole information security context together with physical analysis and its instruments, and the results of vulnerability and risk assessment are omitted. Based on the results of the analysis, the areas for development can be determined.

The Current Status Based on Document Analysis

Both Hungarian expert recommendations and international recommendations have been included in the analysis of information security documents. The Provisional Information Security Rules of the Hungarian Police and the Chapter 10.6 Appendix 'A' of the ISO/IEC 27001:20013 standard regarding network security requirements were used as baseline information security documents.

During the assessment of the current information security status of the police information networks, the above documents were thoroughly analysed. The provisions relating to the information security of information networks are limited in terms of space and time. The analysis regarding the information security of police information networks is restricted in time to the current managerial period of documents made since 2012. Precisely because of these criteria, the purpose of analysing the above mentioned two documents is to reveal information regarding determinations about the current status of information security of police information networks.

Documents including the above mentioned issues include references to the information security of the examined police information networks. However, a lack of administrative measures led to a lack of physical measures. In order to determine these deficiencies, further research of the content of the above examined documents and of the baseline documents is necessary.

Continuing the analysis and determining criteria based on the above, strategically important regulations and relevant information documents are distinguished. Based on these documents made at the managerial level of information system security of the police information networks documents determining information security measures of the examined police information networks and documents influencing those documents can be clearly distinguished.

The first stage of document research is to find regulations relating to analysis of the subject of police information. The acts and decrees listed below were examined from an information security and data security point of view:

- Act CLV of 2009 on the Protection of Classified Information,[2]
- Act IV of 2000 on Information Security, on the Confirmation and Announcement of the 06 March 1997 NATO Agreement in Brussels,[3]

2 Act CLV of 2009 on the Protection of Classified Information.

3 Act IV of 2000 on Information Security, on the Confirmation and Announcement of the 06 March 1997 NATO Agreement in Brussels.

- Government Decree No. 218 of 2011 on the Specific Rules of Acquisition Requiring Classified Information or Measures Concerning the Country's Basic Security, National Security Interests or Special Security Measures,[4]
- Government Decree No. 161 of 2010 on the Detailed Regulations of Classified Information Security and on the Authorisation and Official Supervision of Cipher Activity,[5]
- Government Decree No. 92 of 2010 on the Detailed Rules of Industry Security Verification and of Issuing Site Security Certificate,[6]
- Government Decree No 90 of 2010 on the Rules of the National Security Authority's Operation and of Managing Classified Information,[7]
- Regulations in the subject of data security and information security:
- Act CLVII of 2010 on National Data Property,[8]
- Government Decree No. 38 of 2011 on Securing Data Processing of State Registers Falling Within the Scope of National Data Property,[9]
- Act CXCVI of 2011 on National Assets,[10]
- Act CXII of 2011 on the Right of Informational Self-Determination and Freedom of Information,[11]
- Act CLXXXV of 2010 on Media Services and Mass Communication,[12]
- Act C of 2003 on Electronic Communications,[13]
- Act L of 2013 on the Electronic Information Security of Central and Local Government Agencies,[14]
- Government Decree No. 65 of 2013 (8 March) as the Implementing Regulation of Act CLXVI of 2012 on Identification, Designation and Defence of Vital Systems and Facilities,[15]
- Government Decree No. 301 of 2013 (29 July) on the 'Scope of Duties and Authority of the National Electronic Information Security Authority and of the Information Security Supervisor, and on the Administration Procedure of the National Security Authority',[16]

4 Government Decree No. 218 of 2011 on the Specific Rules of Acquisition Requiring Classified Information or Measures Concerning the Country's Basic Security, National Security Interests or Special Security Measures.
5 Government Decree No. 161 of 2010 on the Detailed Regulations of Classified Information Security and on the Authorisation and Official Supervision of Cipher Activity.
6 Government Decree No. 92 of 2010 on the Detailed Rules of Industry Security Verification and of Issuing Site Security Certificate.
7 Government Decree No. 90 of 2010 on the Rules of the National Security Authority's Operation and of Managing Classified Information.
8 Act CLVII of 2010 on National Data Property.
9 Government Decree No. 38 of 2011 on Securing Data Processing of State Registers Falling Within the Scope of National Data Property.
10 Act CXCVI of 2011 on National Asset.
11 Act CXII of 2011 on the Right of Informational Self-Determination and Freedom of Information.
12 Act CLXXXV of 2010 on Media Services and Mass Communication.
13 Act C of 2003 on Electronic Communications.
14 Act L of 2013 on the Electronic Information Security of Central and Local Government Agencies.
15 Government Decree No. 65 of 2013 (8 March) as the Implementing Regulation of Act CLXVI of 2012 on Identification, Designation and Defence of Vital Systems and Facilities.
16 Government Decree No. 301 of 2013 (29 July) on the 'Scope of Duties and Authority of the a National Electronic Information Security Authority and of the Information Security Supervisor, and on the Administration Procedure of the National Security Authority'.

- Government Decree No. 233 of 2013 (30 June) on the 'Scope of Duties and Authority of the Governmental Incident Handling Centre and Portfolio Incident Handling Centres of Electronic Information Systems; and of the Incident Handling Centres of Vital Systems and Facilities',[17]
- Ministry of Interior Decree No. 36 of 2013 (17 July) on the 'Portfolio Rules of Safety Oversight and Verification of Closed Purpose Electronic Information Systems',[18]
- Ministry of National Development Decree No. 77 of 2013 (19 December) on the 'Requirements of Security Class and Security Level Classification Regarding Technology Security and Secure Information Devices and Products as defined in Act L of 2013 on the Electronic Information Security of Central and Local Government Agencies'.[19]

The second step is to examine regulations determining information security on the portfolio level. The regulations below are highlighted:

- Government Decree No. 1277 of 2010 on the Necessary Measures for Government Information Consolidation,[20]
- Ministry of Interior Instruction No. 12 of 2012 on the Information Strategy of the Ministry of Interior,[21]
- Ministry of Interior Instruction No. 21 of 2011 on the Information Security Policy of the Ministry of Interior,[22]
- Ministry of Defence Instruction No. 94 of 2009 on the Information Security Policy of the Ministry of Defence,[23]
- Ministry of Transport, Telecommunications and Energy Instruction No. 8 of 2009 on the Information Security Rules of the Ministry of Transport, Telecommunications and Energy.[24]

Though the above examined documents are related to the subject of information security of information networks, and can be associated with the police; they do not contain an evident regulation regarding requirements for information security of police information networks. However, all of them can be used to reveal the above mentioned deficiencies.

If we identify the police as a portfolio organisation of the Ministry of Interior, then approaching the question of information security issues of police information net-

17 Government Decree No. 233 of 2013 (30 June) on the 'Scope of Duties and Authority of the Governmental Incident Handling Centre and Portfolio Incident Handling Centres of Electronic Information Systems; and of the Incident Handling Centres of Vital Systems and Facilities'.

18 Ministry of Interior Decree No. 36 of 2013 (17 July) on the 'Portfolio Rules of Safety Oversight and Verification of Closed Purpose Electronic Information Systems'.

19 Ministry of National Development Decree No. 77 of 2013 (19 December) on the 'Requirements of Security Class and Security Level Classification Regarding Technology Security and Secure Information Devices and Products as defined in Act L of 2013 on the Electronic Information Security of Central and Local Government Agencies'.

20 Government Decree No. 1277 of 2010 on the Necessary Measures for Government Information Consolidation,

21 Ministry of Interior Instruction No. 12 of 2012 on the Information Strategy of the Ministry of Interior.

22 Ministry of Interior Instruction No. 21 of 2011 on the Information Security Policy of the Ministry of Interior.

23 Ministry of Defence Instruction No. 94 of 2009 on the Information Security Policy of the Ministry of Defence.

24 Ministry of Transport, Telecommunications and Energy Instruction No. 8 of 2009 on the Information Security Rules of the Ministry of Transport, Telecommunications and Energy.

works, we find concrete references to the field of network security. For example, the Ministry of Interior Instruction No. 12 of 2012 on the Information Strategy of the Ministry of Interior, Chapter IV Strategic Development Areas Sub-Chapter 1 Network Development Policy clearly states: "Efforts should be made to apply modern virtual technologies, which must be supported by establishing a proper data-processing network. Information services must be provided by centralised and integrated systems." It also notes the necessity of establishing physical security instruments, saying that "border firewalls must be established on the information networks of organisations. The organisation must outline the borders of its information network, and must provide every protection within those borders. It must apply such uniformly reliable tools and wholly-owned security procedures which guarantee the safety of data trafficking and storage."

Putting great emphasis on physical security, it underlines that "the server rooms of the Ministry of Interior and its portfolio organisations must be classified into the proper security levels in accordance with the qualification level of the data it stores and its systems. In order to minimise risk margins and increase security, by depreciation replacement it must be attained that all parts of the information equipment are younger than 6 years."[25] These measures weren't contained in the examined documents.

The Ministry of Interior Instruction No. 12 of 2012 on the Information Strategy of the Ministry of Interior document ordains the set-up and management of a documentation system, and states that "to protect the information network of the Ministry of Interior and its portfolio organisations, archiving electric data, creating and managing centrally organised directories, keeping records of access to information systems, logging electronic and paper copying, and printing processes must be focused on the IT domain."[26]

Concrete determinations regarding local networks are also contained: "during the consolidation of local network infrastructure, approximately 4000 new UTP CAT5e network endpoints are set-up (alongside the refurbishment of the already existing 5000 endpoints). Connecting server farms to local networks is going to be guaranteed by Gigabit Ethernet, by homogenising and wholly replacing active devices."

Keeping in mind the above results (which can be efficiently used in developing further police information security documentations), professional standards, based on which further research could be conducted, must be reviewed in order to obtain an accurate understanding of the previously determined points. Unfortunately, in the time period determined above, no further expert directive documents have been created which would have enabled analysis to be continued in the field of network information security. Therefore, the used references of the above documents are examined in order to enable recommendations for correcting other deficiencies. International and Hungarian standards relevant to the analysis of police information network security are clearly identified. See below for the standards actually used:

25 Ministry of Interior Instruction No. 12 of 2012 on the Information Strategy of the Ministry of Interior, p. 14.
26 Ministry of Interior Instruction No. 12 of 2012 on the Information Strategy of the Ministry of Interior, p. 15.

- Bill of 2012 on the Identification, Designation and Defence of Vital Systems and Facilities,[27]
- Recommendation No. 25 Hungarian Information Security Recommendations (Magyar Informatikai Biztonsági Ajánlások, MIBA),[28]
- 25/1. Hungarian Information Security Framework (Magyar Informatikai Biztonsági Keretrendszer, MIBIK),[29]
- Volume 25/1-3. Examination of Information Security Control (Az Informatikai Biztonság Irányításának Vizsgálata, IBIV),[30]
- Volume 25/1-1. Information Security Control System (Informatikai Biztonság Irányítási Rendszer, IBIR),[31]
- 25/2. Hungarian Information Security Assessment and Certificate Scheme (Magyar Informatikai Biztonság Értékelési és Tanúsítási Séma, MIBÉTS).[32]
- International standards used:
- ISO/IEC 27002:2005 and ISO/IEC TR 13335 international standards,[33]
- ISO/IEC 27001:2005 standard,[34]
- ISO/IEC 27001:2013 standard.[35]

According to their relevance, a short summary is made of the importance of standards considered during the analysis:

Recommendation No. 25 Hungarian Information Security Recommendations (Magyar Informatikai Biztonsági Ajánlások, MIBA) was made at the behest of the Central Office for Administrative and Electronic Public Services of the Hungarian Prime Minister's Office. The MIBA's main goal is to facilitate the establishment and maintenance of safe information systems. Conforming to international standards and recommendations, the MIBA has three parts:

The *25/1. Hungarian Information Security Framework* (Magyar Informatikai Biztonsági Keretrendszer, MIBIK)[36] considers the issue of information security from an organisational point of view. Therefore the MIBIK is aimed at leaders responsible for controlling and managing secure information systems, and at experts evaluating the fulfilment of requirements regarding the organisation as a whole.

The *Information Security Guidance for Small Organisations* (Informatikai Biztonsági Iránymutató Kis Szervezetek Számára, *IBIX*)[37] provides advice for organisations lacking a significant information system and a specifically trained information staff with setting up their secure information systems.

27 Bill of 2012 on the Identification, Designation and Defence of Vital Systems and Facilities.
28 Recommendation No. 25 Hungarian Information Security Recommendations (MIBA).
29 25/1. Hungarian Information Security Framework (MIBIK).
30 Volume 25/1-3. Examination of Information Security Control (IBIV).
31 Volume 25/1-1. Information Security Control System (IBIR).
32 25/2. Hungarian Information Security Assessment and Certificate Scheme (MIBÉTS).
33 ISO/IEC 27002:2005 and ISO/IEC TR 13335 international standards.
34 ISO/IEC 27001:2005 standard.
35 ISO/IEC 27001:2013 standard.
36 Hungarian Information Security Framework (MIBIK).
37 Information Security Guidance for Small Organisations (IBIX).

The MIBIK is based on the ISO/IEC 27001:2005, ISO/IEC 27002:2005[38] and the ISO/IEC TR 13335[39] international standards, and the governing EU and NATO regulations.

The Volume 25/1-1. Information Security Control System (Informatikai Biztonsági Irányítási Rendszer, IBIR) is part of the MIBIK, which concerns the planning, maintenance, control and repair of information security. Other parts of MIBIK are the Information Security Control Requirements (Informatikai Biztonság Irányítási Követelményei, IBIK), which provides advice to improve the efficiency of handling information security, enabling a unified method for handling requirements and tasks. The Information Security Control Check (Informatikai Biztonsági Irányításának Vizsgálata, IBIV) provides a methodological assistance for checking information security.

The *Hungarian Information Security Assessment and Certificate Scheme* (Magyar Informatikai Biztonság Értékelési és Tanúsítási Séma, *MIBÉTS*)[40] handles the issue of information security from a technological point of view. Therefore, the MIBÉTS is aimed at leaders responsible for setting up and developing information systems, and experts carrying out the evaluation and authentication of information products and systems security.[41]

Numerous standards and recommendations address the issue of information security. Often the ITIL1[42] and COBIT2[43] are used as references. The ITIL (Information Technology Infrastructure Library) is an internationally recognised document wholly covering information as a service. According to ITIL, security control, though an independent process, is integrated into other processes as much as possible. The Security Management volume of ITIL uses the BS7799[44] standard as reference for expanding ITIL processes with security control. The COBIT is a document known and recognised internationally by information system inspectors, containing guidelines for organizing and especially checking information systems. It puts a great emphasis on security, however, it does not provide detailed elaborations.

The ISO/IEC 15408 standard (Common Criteria)[45] has a predominantly technical approach, and it provides advice mainly for producers of information products. It provides very detailed and reliable requirements and procedures for qualifying the security of information devices. However, it does not provide detailed or adequately developed requirements for organisations operating or using information systems.

Lately the 'technical report' is being increasingly widely used in the context of information security. The ISO/IEC TR 13335 – Guidelines for the Management of Information Security (GMITS)[46] is not a standard, despite being published as a part of the

38 ISO/IEC 27002:2005. standard.
39 ISO/IEC TR 13335. standard.
40 Hungarian Information Security Assessment and Certificate Scheme (MIBÉTS).
41 25/1. Hungarian Information Security Framework (MIBIK) 2008, pp. 5–7.
42 Information Technology Infrastructure Library (ITIL).
43 Control Objectives for Information and Related Technology (COBIT).
44 BS7799.
45 ISO/IEC 15408 (Common Criteria).
46 ISO/IEC TR 13335 – Guidelines for the Management of Information Security (GMITS).

standard series of the International Organization for Standardization and the International Electrotechnical Commission, but instead a 'technical report'. In this case, a technical report provides descriptions of possible solutions, and is only revised once its contents are either invalid or are no longer used. The ISO/IEC TR 13335 consists of five parts:

1. Concepts and models for Information Security,
2. Managing and planning Information Security,
3. Techniques for the Management of Information Security,
4. Selection of Safeguards,
5. Safeguards for External Connections.

"The ISO/IEC 27002:2013 is a crucial standard, because on the one hand it contains information security requirements and defence measures regarding all system components, and on the other hand from among several national documents this is the document that became an international standard, and is also used as a reference by the 'de facto' international standard ITIL. The ISO/IEC 27002 standard – though criticised as well – is accepted as the base of information system security of different organisations around the world, and especially in numerous countries of the European Union. Therefore this international standard should be the basis of current requirements, keeping in mind the ISO/IEC TR 13335 standard and the relevant regulations of the NATO (Security within the North Atlantic Treaty Organisation [NATO] – C-M[2002]49) and the European Union (Security Regulations of the Council of the European Union [2001/264/EK])."[47]

Document analyses in the context of police network information security and protection could not be found in the above outlined structure, neither directly nor indirectly.

Areas for Development

Based on the above it is apparent that police information networks are lacking from an information security point of view and development is necessary.

In determining the areas for development, I drew on the procedural methodology of requirements for technology security, secure informational devices and products, and for the classification of security class and level, which is defined in 'Act L of 2013 on the Electronic Information Security of Central and Local Government Agencies' (hereinafter referred to as 'the ISA' [Information Security Act]) in the framework of the Ministry of National Development Decree No. 77/2013. (19 December) (hereafter referred to as 'the Regulation') and developed by the Hungarian Ministry of National Development. The methodology – concentrating on the sections of the ISA relating to security areas and focusing on three spectrums (confidentiality, integrity and availability) of the police electronic information networks – essentially enables the classification of these networks into five security classes and the determination of areas for development for police information networks. The security areas outlined in the ISA are as follows:

47 Ködmön (2008) 39.

- 'closed protection: protection taking into consideration all possible threats';[48]
- 'comprehensive protection: protection covering all elements of an electronic information system';[49]
- 'continuous protection: uninterrupted protection even under circumstances and conditions which change over time';[50]
- 'protection commensurate with risks: the protection of an electronic information system where the costs of protection are proportionate with the extent of damage which may be caused by the threats'.[51]

The above security areas can be further divided into the following areas:

- Administrative;
- Physical; and
- Logical.

The areas for development can be defined at an organisational level and at the level of police information networks in the scope of the analysed legislation.

Administrative development objectives for the police organisation

Since the ISA is the base document in determining the areas for development, the first administrative development objective concerning police information networks is identified as the security classification of electronic information systems – and thus indirectly of information networks.

According to the general directives of the ISA, "the organisation concerned, in determining the security class of its information system, is to implement commensurately the requirements of confidentiality, integrity and availability having regard to the system's function, therefore for example:

1.1.1. in the case of systems handling national data assets, the requirement of integrity is of the utmost priority;
1.1.2. in the case of vital information system elements, availability is the main requirement;
1.1.3. in the case of special personal data, the maintaining of confidentiality is a fundamental requirement."[52]

48 Act L of 2013 on the Electronic Information Security of Central and Local Government Agencies, Hungarian Official Gazette No. 69 (25 April 2013), p. 50244.
49 Act L of 2013 on the Electronic Information Security of Central and Local Government Agencies, Hungarian Official Gazette No. 69 (25 April 2013), p. 50243.
50 Act L of 2013 on the Electronic Information Security of Central and Local Government Agencies, Hungarian Official Gazette No. 69 (25 April 2013), p. 50242.
51 Act L of 2013 on the Electronic Information Security of Central and Local Government Agencies, Hungarian Official Gazette No. 69 (25 April 2013), p. 50243.
52 Ministry of National Development Decree No. 77 of 2013 (19 December) on the Requirements for Technology Security, Secure Informational Devices and Products and Requirements for the Classification of Security Class and Level as defined in Act L of 2013 on the Electronic Information Security of Central and Local Government Agencies, Appendix 2 Section 1.1, Hungarian Official Gazette No. 214 (19 December 2013), p. 85388.

Taking into account the determinations of the Regulation and Section 9 Paragraph 2 Subsection b of the ISA, according to minimal law requirements I classify the Police as an organisation as Security Class Level Three. This classification means that the Police as an organisation has no system with a higher security classification than Level Three, and "the organisation concerned requires its electronic information security processes to be soundly regulated, the processes to be documented and the administrative security measures to be supported with effective logical security measures."[53]

In a broader sense this definition means in the case of the Police that "the security processes of electronic information systems are determined and are harmonised with information security policies and information security regulations."[54]

Derived from the above, the apparent main objective for the Police is to lay down and – according to the requirements applicable to the organisation concerned – to document and to announce the information security strategy within the organisation, which sets out the method, instruments and schedule of realising security policy objectives. The information security strategy has to lay down objectives in the short, medium and long term, which ensures a fully-fledged security framework for the organisation. An additional potential objective is to determine the frequency of supervising and updating the information security strategy in the context of internal regulation of the information security strategy itself, thus guaranteeing the basic principal of continuity.

Furthermore, the Regulation requires that "the responsibilities relating to electronic information systems are determined and stakeholders are familiar with and agree to them."[55]

Interpreting this standard in the context of the Police, the tertiary objective for the Police is to ensure that no unauthorised entity can obtain information on or modify the information security strategy. The information security strategy of the organization concerned should be harmonized with its other strategies (especially relating to budgetary and human resources planning, and changes in scope of activity and development) and with its vision.

Moreover, the Regulation is permissive in this regard, since it only spells out as an expectation for the organisation concerned – the Police – to "implement and to demand security awareness, to conduct security training in informational and general

53 Ministry of National Development Decree No. 77 of 2013 (19 December) on the Requirements for Technology Security, Secure Informational Devices and Products and Requirements for the Classification of Security Class and Level as defined in Act L of 2013 on the Electronic Information Security of Central and Local Government Agencies, Appendix 2 Section 2.1, Hungarian Official Gazette No. 214 (19 December 2013), p. 85392.

54 Ministry of National Development Decree No. 77 of 2013 (19 December) on the Requirements for Technology Security, Secure Informational Devices and Products and Requirements for the Classification of Security Class and Level as defined in Act L of 2013 on the Electronic Information Security of Central and Local Government Agencies, Appendix 2 Section 2.1, Hungarian Official Gazette No. 214 (19 December 2013), p. 85392.

55 Ministry of National Development Decree No. 77 of 2013 (19 December) on the Requirements for Technology Security, Secure Informational Devices and Products and Requirements for the Classification of Security Class and Level as defined in Act L of 2013 on the Electronic Information Security of Central and Local Government Agencies, Appendix 2 Section 2.3.2, Hungarian Official Gazette No. 214 (19 December 2013), p. 85392.

professional areas, but the scheduling and way of conducting this training is not formalised."[56] Thus it does not regulate every aspect of security.

The Regulation differentiates between the following administrative security areas:

- Basic tasks at an organizational level;
- Risk Assessment;
- Design;
- Procurement of Systems and Services;
- Security Analysis;
- Personal Security; taking into account the human factor; and
- Awareness and Training.

These general security areas have to be realised at an organisational level, have to be understood for the whole organisation, and in the case of police information networks, can only be applied indirectly.

Further security tasks could be added to the above areas and with those tasks further procedures and documentation as well. Based on an analysis of available police documentation and legal compliance, the conclusions are the following:

- Documentation doesn't lay out procedures or areas for police information networks;
- In practice, there is an obvious lack in developing the above procedures or having outcomes from the above administrative activities; and
- Tasks concerning the above areas are not determined.

Development objectives for the physical security area

In determining objectives for the physical security area, based on the guidelines laid down in the Regulation (considering the organisation in question is a law enforcement organisation), the three-level security classification can be applied.

In this case of analysing the physical security area, systems which are part of police information networks, but are above security class Level Three at the Police as an organisation, are not considered.

Following this conclusion, in the case of this classification, the Regulation requires "physical security measures to comprise overseeing physical accesses to information system elements and that physical parts of the system are protected from potential physical harms by applying further protective measures."[57] Of course, this requirement assumes that the organisation – in this case the Police – has already carried out a risk assessment, and is fully aware of the threats to the police information networks.

56 Ministry of National Development Decree No. 77 of 2013 (19 December) on the Requirements for Technology Security, Secure Informational Devices and Products and Requirements for the Classification of Security Class and Level as defined in Act L of 2013 on the Electronic Information Security of Central and Local Government Agencies, Appendix 2 Section 2.3.6, Hungarian Official Gazette No. 214 (19 December 2013), p. 85392.

57 Ministry of National Development Decree No. 77 of 2013 (19 December) on the Requirements for Technology Security, Secure Informational Devices and Products and Requirements for the Classification of Security Class and Level as defined in Act L of 2013 on the Electronic Information Security of Central and Local Government Agencies, Appendix 2 Section 2.3.7, Hungarian Official Gazette No. 214 (19 December 2013), p. 85392.

Among the requirements, the Regulation emphasizes the importance of availability, which assumes in the case of this classification that "auxiliary jobs are created or are available as determined by the organisation concerned."

In the case of Level Three classification, an additional, strategic requirement is "to seek security evaluation or audit of the integrated electronic information system during the development of electronic information systems."

During analyses of police information security documentation, the documents evidently did not contain the requirements outlined above. In conclusion, the remedy of deficiencies concentrating on the following areas was identified as an objective:

- Risk Assessment;
- Monitoring Physical Threats;
- Creating Auxiliary Jobs; and
- Establishing an Audit System.

Development objectives for the logical security area

As in the above case, in determining objectives for the logical security area, based on the guidelines set in the Regulation, the Level Three security classification systems are examined. In analysis of the logical security area, systems which are part of the police information networks, but are above security class Level Three at the Police as an organisation, are not considered.

Upon examining this area, the Regulation gives priority to "protection commensurate with risks". This means that the costs of protection are proportionate with the extent of damage which may be caused by any threats. Again, the assumption that the requirements demand decision-making based on risk assessment reappears. During the process of security classification the Regulation assumes that "the results of the risk assessment are considered upon developing security solutions",[58] in this current case, in the case of police information networks. This requirement clearly shows that conducting risk assessments is crucial for realising the development objectives.

However, there is no expectation of full implementation among the requirements. This fact is furthermore supported, because "safety management goals and measurement methods are determined, however, are not fully applied".[59] This wording assumes a suspensive character of the implementation, which gives further possibilities in a forward-looking fashion to create new security objectives in the area of full implementation.

58 Ministry of National Development Decree No. 77 of 2013 (19 December) on the Requirements for Technology Security, Secure Informational Devices and Products and Requirements for the Classification of Security Class and Level as defined in Act L of 2013 on the Electronic Information Security of Central and Local Government Agencies, Appendix 2 Section 2.3.3, Hungarian Official Gazette No. 214 (19 December 2013), p. 85392.

59 Ministry of National Development Decree No. 77 of 2013 (19 December) on the Requirements for Technology Security, Secure Informational Devices and Products and Requirements for the Classification of Security Class and Level as defined in Act L of 2013 on the Electronic Information Security of Central and Local Government Agencies, Appendix 2 Section 2.3.4, Hungarian Official Gazette No. 214 (19 December 2013), p. 85392.

Moreover, the Regulation consistently applies feedback in every aspect of security procedure. This security feedback mechanism appears on this classification level as well: "occasional safety tests and vulnerability tests are conducted".[60]

During analysis of the logical security area, the fact that the minimal requirements determined by legal norms are not apparent in the normative regulation in the case of the police information networks came to light. Therefore, the logical security area development objectives are as follows:

- Risk Assessment;
- Development of Safety Solutions;
- Determination of Measurement Methods;
- Tests; and
- Vulnerability Analysis.

Summary

The aim of this examination was to identify areas for development by examining the information security context of police information networks.

Based on the analyses' results on the information security context of information networks, the information security status of police information networks could be determined.

The aim of examining the documents was to identify expert directives referring to the information security status of police information networks. Documents dealing with the identified subjects contained references relating to the information security of police information networks were considered in the examination.

With regard to the above, the carried out examination required analyses concentrating on several areas in a long span of time. The analyses was conducted with regard to the vastness of the information network of the police. The primary starting point was the current situation. This analysis took into account relevant Hungarian and international recommendations. The Provisional Information Security Rules of the Hungarian Police and the Chapter 10.6 Appendix 'A' of the ISO/IEC 27001:20013 standard regarding network security requirements were used as baseline documents during the analysis of network information security requirements.

The research focuses were identified as assessment, examination of security classification, existing measures, applicability of regulations and physical feasibility.

19 laws and legislative decrees were examined and analysed, looking for references to information security and relevant data security, during which the context of the information security of police information networks was researched.

This producing no results, a further five regulations determining information security on the portfolio level were reviewed. These touched on the subject of information

60 Ministry of National Development Decree No. 77 of 2013 (19 December) on the Requirements for Technology Security, Secure Informational Devices and Products and Requirements for the Classification of Security Class and Level as defined in Act L of 2013 on the Electronic Information Security of Central and Local Government Agencies, Appendix 2 Section 2.3.5, Hungarian Official Gazette No. 214 (19 December 2013), p. 85392.

networks and information security, and could be related to the police. Furthermore, they contained precise determinations regarding the increase of the network information security level, which can provide assistance in outlining the requirements for the information security of police information networks. Therefore, in extending research to expert resources, eight Hungarian and international standards were identified.

Alongside theoretical examinations, practical realisation was also dealt with in the context of the description of police information networks. During these examinations it became obvious, that police information networks were not classified, and therefore the circumstances of classification could not be examined.

Summarising the above, information security can be considered underdeveloped both from an administrative and information security measures point of view. With a lack of adequate regulation, the classification level of the police information networks could not be determined. No documents were found which would have referred to security classification or its information security situation, risk analysis, risk management, procedures or measures. This pointed to a series of deficiencies, which provided evidence that information security regulations, measures, procedures and their physical feasibility are indispensable. Deficiencies revealed at each stage of the examination proved a cause and effect relationship among the examined points, meaning that deficiencies in one point led to deficiencies in the following examined point. However, among regulations relevant to the domain, apparent references and definitions could be identified, processed and used to develop the information security level of police information networks. Applying these regulations, documentation can be developed to enable determination of the security classification of police information networks. Furthermore, by extending the circumstances of classification, measures and procedures can be developed to minimise information security risks.

On the basis of the above regulations the information networks of the police were classified. Taking into account the Security Class Level Three organisational level classification, based on the security measures in the spectrum of confidentiality, integrity and availability, the areas for development were determined. During the examination, the fact that the police information systems have no system with a higher security classification than Level Three, was considered a basic fact. In order to realise the categorised objectives, measures in line with the decree must be determined. The order of realising these measures must be recorded in an action plan.

This analysis covered the guidance table in the Annex of the Regulation, a 1700 question survey, which helped to determine security classes as laid down by the Hungarian National Electronic Information Security Authority, and the manual made by the Hungarian Central Office for Administrative and Electronic Public Services. Based on these analyses, the most important range of measures for the police to implement were outlined. The range of measures were prepared based on determinations in Annex 3 and 4 of the 'National Security Authority Regulation No. 77/2013. (19 December) on the Requirements for Technology Security, Secure Informational Devices and Products and Requirements for the Classification of Security Class and Level as defined in Act

L of 2013 on the Electronic Information Security of Central and Local Government Agencies'. Based on that, the following developments to protect the police information network were determined:

During the development the range of measures has to be laid down in the following rules:

- Organisational level basic tasks have to include the following regulations:
  - Risk Assessment;
  - Design;
  - Procurement of Systems and Services;
  - Security Analysis;
  - Personal Security; taking into account the human factor; and
  - Awareness and Training.
  - Physical security procedure has to include the following regulations:
  - Physical Entry Authorizations;
  - Supervision of Physical Accesses;
  - Checking of Visitors;
  - Emergency Lighting;
  - Fire Protection;
  - Monitoring Temperature and Humidity; and
  - Delivery and Transport.
- Logical security procedure has to include the following regulations:
  - Configuration Management;
  - Planning of Business-as-usual;
  - Maintenance;
  - Protection of Data Carriers;
  - Identification and Authentication;
  - Verifying Access;
  - System and Information Integrity;
  - Logging and Accountability;
  - System and Communication Protection; and
  - Response to Security Incidents.

Conclusion: there is an evident cause and effect relationship between links of the chain of the information security of the examined systems and measures as determined as a result of security level classification and procedures. The breaking of this chain creates an obvious cause and effect chain reaction. These cause and effect relations result in a risk of IT information security threats.

REFERENCES

Act IV of 2000 on Information Security, on the Confirmation and Announcement of the 06 March 1997 NATO Agreement in Brussels
Act L of 2013 on the Electronic Information Security of Central and Local Government Agencies, Hungarian Official Gazette No. 69 (25 April 2013)
Act C of 2003 on Electronic Communications
Act CLV of 2009 on the Protection of Classified Information
Act CLVII of 2010 on National Data Property
Act CXII of 2011 on the Right of Informational Self-Determination and Freedom of Information
Act CLXXXV of 2010 on Media Services and Mass Communication,
Bill of 2012 on the Identification, Designation and Defence of Vital Systems and Facilities
Act CXCVI of 2011 on National Assets
BS7799
Control Objectives for Information and Related Technology (COBIT)
Examination of Information Security Control (Az Informatikai Biztonság Irányításának Vizsgálata, IBIV)
Government Decree No. 38 of 2011 on Securing Data Processing of State Registers Falling Within the Scope of National Data Property
Government Decree No. 65 of 2013 (8 March) as the Implementing Regulation of Act CLXVI of 2012 on Identification, Designation and Defence of Vital Systems and Facilities
Government Decree No. 90 of 2010 on the Rules of the National Security Authority's Operation and of Managing Classified Information
Government Decree No. 92 of 2010 on the Detailed Rules of Industry Security Verification and of Issuing Site Security Certificate
Government Decree No. 161 of 2010 on the Detailed Regulations of Classified Information Security and on the Authorisation and Official Supervision of Cipher Activity
Government Decree No. 218 of 2011 on the Specific Rules of Acquisition Requiring Classified Information or Measures Concerning the Country's Basic Security, National Security Interests or Special Security Measures
Government Decree No. 233 of 2013 (30 June) on the 'Scope of Duties and Authority of the Governmental Incident Handling Centre and Portfolio Incident Handling Centres of Electronic Information Systems; and of the Incident Handling Centres of Vital Systems and Facilities'
Government Decree No. 301 of 2013 (29 July) on the 'Scope of Duties and Authority of the National Electronic Information Security Authority and of the Information Security Supervisor, and on the Administration Procedure of the National Security Authority'
Government Decree No. 1277 of 2010 on the Necessary Measures for Government Information Consolidation
Hungarian Information Security Assessment and Certificate Scheme (Magyar Informatikai Biztonsági Értékelési és Tanúsítási Séma, MIBÉTS)
Hungarian Information Security Framework (Magyar Informatikai Biztonsági Keretrendszer, MIBIK), 2008.
Information Security Control System (Informatikai Biztonság Irányítási Rendszer, IBIR)
Information Security Guidance for Small Organisations (Informatikai Biztonsági Iránymutató Kis Szervezetek Számára, IBIX)
Information Technology Infrastructure Library (Information Technology Infrastructure Library, ITIL)
ISO/IEC 27002:2005 and ISO/IEC TR 13335 international standards
ISO/IEC 27001:2005. standard
ISO/IEC 27001:2013. standard
ISO/IEC 27002:2005. standard
ISO/IEC TR 13335. standard

ISO/IEC 15408 (Common Criteria)
ISO/IEC TR 13335 – Guidelines for the Management of Information Security (GMITS)
Ködmön István: *Information Security Reflecting The ISO27001 Standard, Top Secret Stories*, Hétpecsét Information Security Association, Budapest, 2008. [unofficial translation] (Dr. Ködmön István: *Információbiztonság az ISO27001 tükrében, Hétpecsétes Történetek*, Hétpecsét Információbiztonsági Egyesület, Budapest, 2008.)
Ministry of Defence Instruction No. 94 of 2009 on the Information Security Policy of the Ministry of Defence
Ministry of Interior Decree No. 36 of 2013 (17 July) on the 'Portfolio Rules of Safety Oversight and Verification of Closed Purpose Electronic Information Systems'
Ministry of Interior Instruction No. 12 of 2012 on the Information Strategy of the Ministry of Interior
Ministry of Interior Instruction No. 21 of 2011 on the Information Security Policy of the Ministry of Interior
Ministry of National Development Decree No. 77 of 2013 (19 December) on the Requirements for Technology Security, Secure Informational Devices and Products and Requirements for the Classification of Security Class and Level as defined in Act L of 2013 on the Electronic Information Security of Central and Local Government Agencies, Hungarian Official Gazette No. 214 (19 December 2013)
Ministry of Transport, Telecommunications and Energy Instruction No. 8 of 2009 on the Information Security Rules of the Ministry of Transport, Telecommunications and Energy
Recommendation No. 25 Hungarian Information Security Recommendations (Magyar Informatikai Biztonsági Ajánlások, MIBA)

ABSZTRAKT

A rendőrségi informatikai hálózat információbiztonsági fejlesztési irányai

FEHÉR JUDIT

Az információbiztonság helyzetéről készülő felmérés a biztonság, az irányítás és a kockázatkezelési területek helyzetéről adhat egyszerre objektív és átfogó képet. A hálózat információbiztonsági hátterének meghatározásához, a valós értékek eléréséhez meg kell vizsgálni a hálózathoz tartozó dokumentumokat, az informatikai rendszerek és a hálózat lehetséges fenyegetéseit, veszélyhelyzeteit. A rendőrségi informatikai hálózatok védelmét a törvények szerint a rendőrségnek garantálnia kell, ezért a fejlesztési irányokat az adminisztratív, a logikai és a fizikai területekre kell koncentrálni. Az irányvonalakat szervezeti szinten és a rendőrségi informatikai hálózatok szintjén lehet meghatározni. Az irányvonalak segítségével körvonalazódik azon feladatok és egyben intézkedések köre, amelyek segítségével elérhetőek a védelmi stratégiai célkitűzések és teljesíthetőek a követelményrendszerek.

Kulcsszavak: *információbiztonság, biztonsági osztály, stratégia, intézkedések, adminisztratív, fizikai, logikai*