9

A strategic approach to a national security policy

Zeger, Hans G.
ARGE DATEN - Österreichische Gesellschaft für Datenschutz
(Austrian Society of data protection and privacy)
A-1170 Wien, Sautergasse 20, Austria. ☎ +43/1/4897893,
Fax +43/1/4897893-10, 🖃 hans@email.ad.or.at

Abstract

IT-security policy can be understood as a union of targets and actions to realize the essential security principles "confidence", "availability" and "integrity" of information processing in the best systematic and balanced way as possible. For the further practical realization of this security policy, evaluation and certification proceedings have to be requested.

This inquiry was presented in winter 1994. On the one hand it illustrates a high general consciousness for problems of information security among Austrian information processing organisations. On the other hand, due to the lack of a national security policy, there is a deficiency of practical translation and orientation to exactly defined security goals.

The intention of this paper is to present arguments for the necessity of a national security policy. This makes sense regarding the increasing number of policy-neutral certification methods like [ITSEC], as well as in view of the efforts to realize security requirements in a more technical than a legal or administrative way. This is also of importance considering the international orientation of the development of information systems.

This particular national position should not diverge from international positions, goals and standards, but it should offer a possibility for Austria to participate in this international discussion as an equal partner. This will be of interest for individuals as well as for commerce. It means advantages in competition for Austrian producers of information systems and it also means advantages for Austrian consumers of information products in the fields of law enforcement, service and product liability and guarantee of quality.

Keywords

information security, security policy, privacy, data protection, evaluation, certification, Austria, European Community.

R. Posch (ed.), *Communications and Multimedia Security*

1 INTRODUCTION

Security-policy means a consistent approach to the security risks and threats, the basic requirements of information processing, the sensitivity of data and the resulting security activities in a specific branch, a specific business or any other field of interest.

Different classes of sensitivity of processed information, different complexity of data processing and different usage and access to information are as important as the economic, social and legal framework.

In consideration of all these points an overall reference model, called security policy, can be deduced, which has to be adapted inndividually to a specific user or usage. An objectivated approach of that security policy consists of well known certification and evaluation models as well as legal enforcements for data-processing or comparable institutions and of job descriptions.

If security policy is absent, deficient or inadequate, a generally accepted consensus about security risks and threats as well as about requirements in developing and operating of information systems cannot be found.

In such a context information systems are seen as systems which have to be protected against a vaguely defined hostile enviroment. This situation - to take care against a broad spectre of threats without concern of real risks makes security investments unneccesary expensive and ineffective. On the other hand, inadaequate security activities may restrict the necessary integration of information services.

The first goal of the presented inquiry was to check out the institutional framework for security policy in Austria. The second goal was to gain knowledge about the expectations of customers of information systems with regard to security policy and to collect information about the organisational enviroment of the user.

The last part of this paper explains the advantages and the needs of a national security policy in Austria.

2 INTERNATIONAL

The evolving point of security-policy was by realizing that security of information systems cannot only be a matter of abstract definition but has to be regarded in conjunction with reasonable scenarios of safety and confidence. The idea to define security policies as basic principles of trusted computing can be found at the beginning of the Eighties, starting in 1983 with the "orange book" [TCSEC]. Different levels of security are defined to accomplish different security demands.

In the following years a number of security concepts werde developed by Canada, Germany, France, the United Kingdom, as well as by ISO and NATO. See Table 1.

Table 1 The evolvement of Evaluation Criteria in IT-Security

date	USA	Canada	BRD	GB	F	EU	Int.
1983	TCSEC, 1.Entwurf						
1984							
1985	TCSEC	CTCSEC, Version 1					
1986							
1987							NATO-TCSEC
1988							OSI/ISO 7498-2
1989			ZSIEC	CESG3	SCSSI		
1990						ITSEC, 1. Version	
1991						ITSEC, Version 1.2	
1992	FC, Version 1						
1993		CTCSEC, Version 3					
1994							CC

Thus vendors and users of information systems were confronted with a variety of different policies and methods. The question arose, which of these concepts should be put into realization, as the observance of every one of these was causing enormous costs. For instance the costs of evaluating the operating system 'BS 2000 Rel.10' by Siemens amount to 4.6 million DM, compared with the total costs of system development of 20.3 million DM.

The situation was tightened up by the fact, that requirements concerning confidence and secrecy strenghtened by military applications do not gain a comparable importance in civil or commercial services. A system considered as secure in a military environment is not necessarily an adequate system for the fulfilment of tasks in banking or medical service or governmental administration.

These first experiences with security policy and the paradoxon to discuss and regulate a matter publicly which was considered to be clandestine and confidential in the opinion of most computer experts led to a series of activities in the European Community:

(1) The foundation of a EC-wide security-group, the Senior Officials Group for Information Systems Security [EUSEC], to coordinate the security efforts in governmental administration.
(2) The recommendation to establish a department for security and evaluation in every country of the EC.
(3) The development of an EC-wide general framework for the definition of security and evaluation [ITSEC, ITSEM].

(4) Developing a scale of special directives for the fields of privacy [EUDSR], of free data flow within the EC and of telecommunication [ISDN].

These provisions should encourage vendors and users of information technology to orientate their systems to these goals: "A consistent approach at European level could help to promote the interoperability of systems, lower existing barriers and avoid the formation of new ones between the individual member states and with other countries in compliance with the competition rules and the internal market policies." [GREEN94, p.11].

On the other hand, information technologies, evaluated against the criteria of the European Community should participate at the advantages of competition. The fragmentation of evaluation methods and security policies should be overcome, the individual and customer should sufficiently be protected against the risks of information technique.

3 AUSTRIAN POSTION AND ACTIVITIES

The Austrian Data Protection Law (Datenschutzgesetz) [öDSG] declares a clear intention towards security in information techniques. But this position is not enforced by any organisation, person or institution. This situation implies a conflict between the classical approach cocerning safety and avoidance of computer abuse versus the targets of privacy and individual data protection, as described in FISCHER-HÜBER [SIS-FI].

Eighteen years after the issuing of the Austrian Data Protection Law this fundamental conflict of contradicting security policies still dominates the relation between data processors and users of information systems on the one hand and the data subjects on the other hand. The guidance lines of the Austrian Data Protection Law are not considered helpful, neither by IT-service providers ("too bureaucratic") nor by the data subjects ("no efficent way to enforce the personal privacy rights").

This not at all sufficiently discussed conflict of different security policies leads to the result that the Austrian Data Protection Law is regarded to be a "dead law", meaning to be unapplicable in most vital concerns.

The lack of specialized data protection commissioners in most of the computer centres and the absence of an applicable job description for the tasks of a "data protection commissioner" is also an obstacle towards an experienced discussion about the national security policy.

Thus, we can only list a number of isolated and rather inefficient activities in Austria.

- The dimension "privacy of data"is characterized by a high amount of bureaucracy (the need to register data processing systems without any attendent or supporting supervision).
- In the central information concept of the Austrian Government, called "Informatik Leitkonzept", the term IT-security is only found in connection with the scope of duties of the federal chancellor bureau ("Bundesministeriengesetz").
- The participation of the federal chancellor bureau in the Senior offical group of information security (EC).
- It-security is seen as an internal affair of the nine federal countries.
- There is no accredited institution that is specialized for evaluation, certification and advise in information security techniques.
- The only institution with the capability of system security checks in the governmental sector is the Austrian Data Commission ("Datenschutzkommission"). Due to the minimal personal

staff, this commission performed only six (!) security checks in the years 1991-1993, 18 procedures are not yet finished, the number of open procedures is increasing.

- The federal chancellor Vranitzky delegated the security competence in his speech at Alpbach[VRAN] to the data protection concil ("Datenschutzrat"), a board that was originally founded in the data protection law to comment and supervise the privacy rigths in new legislation outlines.
- In the governmental sector of IT-processing something like common criteria [CC94] can be found in the so called "Datenschutzverordnungen", special regulations for every Ministery or governmental sector to involve specific data-protection and data security rights.
- In the area of financial services (like banking) there is a common approach in the definition of the minimal efforts of security in home-banking.

4 ITSEC'94 - AN INQUIRY

The inquiry was based on a questionnaire and additional interviews and should form an overview about the situation concerning IT-security in Austria.

The results of this study are nevertheless limited due to two conditions:

a) Data processors in Austria - as well as in other countries - don't like to talk about security activities.
b) In Austria there is no requirement for a commissioner of data protection in the companies and administrations. Therefore some small and medium sized companies are unable to answer the large and time consuming questionnaire.

The first part of the questionnaire consists of questions about the own security practice. The second part includes more general questions about an Austrian IT-security-policy.

377 organisations have been contacted (companies, governmental and non-governmental administrations), nearly in the relation 1:1 between private and governmental organisations.

45 questionnaires were returned, 20 of them from governmental, 20 from private organisations, 5 were sent back anonymous. Half of the participants answered the question about the number of employees. The average size was 1800. The organisations are asked about the significance of information technique in their own organisation. The answer could be put into a 100-point scale (with 100 as maximum = information technique is absolutely necessary for the functioning of the organisation). One half of the participants answered with values between 90 and 100, only 2 answered with values below 50, 3 did not answer this question, the remainder answered with values between 50 and 90.

Generally can be stated, that this inquiry covers a small, but highly motivated fraction of Austrian data processors.

5 PART I: SECURITY PRACTICE

Question 1: What terms are associated with "IT-security"?

- Each of the terms "safety" (defined as protection against loss of data), "privacy" (as human right), "security" (defense of computer abuse) and "integrity" (keep an information system consistent) are correlated with the term "security policy" by more then 2/3 of the participants of the questionnaire.

- Only the term "quality" (in the meaning of quality of information system) was correlated with less than 50% of the participants.

A pleasing result was the high priority of the term "privacy" in context with IT-security. This can be interpreted as a mandate to the legislator to consider privacy requirements in every regulation of information techniques.

Question 2: Is there any consensus about the criteria of a secure information system?

- The basic security terms "confidence" (100% consent), "availability" (96%) and "integrity" (93%) are also the top-requirements for Austrian responsibles for information technique.
- The chances of formal verification methods in Austria are relatively small. Less than 50% would use formal verification to examine an information system as a secure system.

In case of legislative regulations, this is interpreted as a mandate for a more general security policy compared to the actual state that can be found in regulations like "Datenschutzgesetz" or the prosecution of computer crime in the penal law ("Strafgesetz"). These regulations only reference to the term "confidence" and the breaking of this "confidence" by a penetrator from outside of the information system.

Question 3: What security activities should be realized and are already realized?

- The questionnaire offered 33 different activies (organisational, software and hardware related and site structural oriented activitites). The answers show a broad bandwith of activities, only two actions are classified as "exotic":
  - insurance against loss of data (13 answers of 45 participants)
  - auditing of ALL data-calls (reading of data) (9 of 45))
- Top security activities are "Backups" (100% consent) and protection against fire hazards (93% consent). Both are typical "safety"-activities.
- On the same activities the questionnaire shows big differences between consent and practice. These activities are considered as important but are not realized internally:
  - Publishing an own IT-guideline for emergency cases (35 consent, 9 realisations)
  - Publishing an own IT-security guideline (28 consent, 8 realisations)
  - Encoding of data and/or data-transfer (25 consent, 7 realisations)
- Auditing of the whole operational activities of the information systems, which is essential in tracking down security gaps, was rarely encountered.
- Of relatively high importance was the activity "Selection of HW- and SW-components with integrated security function" (84% consent).

Less interest was found for prospective security activities, like auditing, yet more for defending activities, like protection against fire. And there is a good chance for new IT-Products, like HW- and SW-components with integrated security functions. But this interest in more integrated security technology is limitated by the costs.

Question 4: Who is / Who should be responsible for IT-security?

- 53% of the participants claim that the management of the data processing department is responsible for IT-security. But only in 7 cases the management is in fact responsible.
- 3/4 of the participants state, that the data processing department (or part of it) is responsible for IT-security. Only in 1/3 of the cases the department is really responsible.

This difference between claimed and effective responsibility might be seen in conjunction with the missing professional profile for a "commissioner for data protection" in Austria.

Question 5: How is the observance of IT-security checked?

- On top of checking the observance of IT-security are periodical instructions of the employees (80%) and directions of the management (67%).
- Effective supervision is generally requested (90% consent) but not generally realized (50% do it in their own organisation).
- Internal revisions or the analysing of auditing protocols without announcement are very popular (80% consent) and more often realized (40%) than originally assumed.

There is a general willingness to the use of effective supervision methods, like revision, protocolling, ... but there is a gap to realize it. In a future regulation of security policy, there should exist some benefits for data processors to do some of this supervision actions.

Question 6: What Methods should be used / are used to check the own IT-security?

- On top of all aids 71% called the security requirements of the öDSG (Austrian data protection law) as most popular way towards better IT-security. This ist rather suprising, because the öDSG contains only a very small number of principles concerning data security as the main issue if it is to protect the privacy of data.
- On the second rank are organisation specific security checklists (67%).
- International methods of evaluation of security of information systems are well known by the participants. More than 80% of the participants say that the use of international evaluation methods is desirable, but only 10% use them in their own organisation.
- 37% use objectivated evaluation methodes, e.g. security guidelines from international standard organisations, recommendations of HW/SW-suppliers or different international guidelines like ITSEC from EC or the "Orange Book" of the DoD.

Each organisation, that uses at least one method of evaluation of security is using more than one method. There is no single or specific method for the evaluation of IT-security in Austria.

Question 7: For which security products is there a market in AUSTRIA?

- The participants of this questionnaire would accept additional costs for additional protection of Personal Computers, for better password security and user identification at the terminals

(84%), and for increased security of existing security measurements, e.g. doors (71%), datasafes (71%), access control systems (69%).
- For cryptographic methods there is at the time no market in Austria. 40% of the participants can imagine to pay extra money for cryptographic software, but only 25% would pay additional money for cryptographic hardware. It is possible that there is a general lack of information about the costs and the effectiveness of such security protection methods.

In general the user of information systems prefer to improve already well known security activities to installing new and additional security utilities.

To make cryptographic methods a widely used product in Austria, it is necessary to enhance the information of the operators of information systems, especially regarding the possibilities to integrate this methods in their own system. This task cold be accomplished best by an independent research institute.

6 PART II: QUESTIONS ABOUT AN AUSTRIAN SECURITY POLICY

Question 8: What is the position of Austria in participating in an international security policy?

- Only 38% of the participants wish a more active cooperation from Austria to formulate an international security policy.
- 70% (both private and governmental organisations) mean that the Austrian data commission (DSK) is a possible and/or desirable representative of Austria [DSK93].
- Small competence in IT-security are given the Autrian Postal-and Telegraphic-Company (PTV), the federal chamber of commerce or the Ministery of economic affairs.

The participants set a high amount of confidence in advance into the Austrian data-commission (DSK), but this is not quite justified regarding the personal and organisational situation of this organisation. The DSK was originally founded to judge specific questions concerning the privacy of data in governmental organisations.

The answers of these questions show that there is an enormous lack of a competent organisation to formulate a comprehensive Austrian security policy.

Question 9: Should there be different security requirements in different social and economic fields?

- The majority of the participants say that special regulation for IT-security is needed in different special fields like national security, financal services, governmental administration, religion and so on (between 62% - 80% depending of the field).
- In summary 87% of the participants mean, that specific fields should have specific regulations, but only 47% mean their own field should be submitted to specific regulation.

There is a gap between the risks of information processing seen at the other data processors and the assessment of the risks of the own data processing. Shortly said: Security risks are the risks of the OTHER data processors. Future regulations should have mechanisms to objectivate the status of security of a given data processing system.

Question 10: What political action should be taken to have better IT-security in Austria?

- On the top of the answers was the desire for a special training (graduate or post-graduate). 91% wanted more consideration of IT-security in the studies of computer science. 78% wanted a better (by meaning professional) supply of IT-security-tutorials and meetings.
- Second, the offerer of secure / certificated IT-products should have economic advantages. 60% wish a preference of certificated products in public tenders.
- Less popular are licensing and supervision authorities (only 31% consent). This is in contrast to the efforts of the European Community to force national and international certification institutions like the "Bundesamt für Informationstechnik" [ITSHB] in Germany.
- Also less popular are "strong legistic regulations of IT-security without criminal penals" (only 31% consent). This reflects exactly the situation in the Austrian data protection law. More consent can be found in the position "strong legistic regulations of IT-security WITH criminal penals" (53%).

7 SUMMARY TO THE QUESTIONNAIRE

- In Austria a high general consent to security in information technology can be found, but there is a lack to formulate clear and distinct security policies.
- By now there is no uniform and on general consent based Austrian security policy. Rudiments are found in special fields like the financal sector, e.g. in the home-banking sector.
- The actually used legistic regulations, like data protection law have not withstood the test. New regulations should increase the support of good security techniques and should punish security lacks.
- On international activities in this field Austria can be seen rather as a spectator than a competent cooperator.

8 WHY A NATIONAL SECURITY POLICY?

In face of the tendencies of an increasing number of international license and evaluation methods, also in face of an international orientation in developing and marketing of IT-products, it may be a national luxury to have own ideas and positions in security policy.

In fact, there are some good practical and economic reasons to do an independent task in security policy.

- An Austrian security policy expresses the national information policy of governmental authorities, like a "freedom of information act" that should regulate the access to confidential and non-confidential information sources.
- It will also regulate the guarantees and demands of users of information services against information providers, like financial services, banking services, home-shopping services and so on.
- Furthermore should be regulated the relation between the requirements of national security (like law enforcement, unlimited access to information sources for investigations against organised crime).

- A national evaluation- and advisory board, based on an national security policy gives Austrian manufactors and developers of IT-security-products the chance to have quick and privileged certification of new products. This could be an enormous advantage in competition .
- Data processors can orientate the evolvement of their information systems and their security activities on a consistent security policy. Consumers and persons, which are confounded from information technologies have an unbureaucratic advisory board in question of good, meaning secure information system and data processing praxis. This board might be an informal instituion to check the security of typical consumer systems, like home-banking, electronic mailboxes or accounting of telephone charges.
- A national consensus about information security policy is a significant precondition that Austria is able to participate in the international discussion as an equal partner.
- In face of the new European data-protection directive with the explicite necessity to declare the applied security methods and standards at the installation of a new data-processing system and with special facilitations for administrations with their own data-protection-commissioner, there is the need of quick response for Austrian data-processors and the legislation.
- The potential conflict between strong security methods, used in buissness and commerce, with the potential abuse through organised crime and the demands of national security in law enforcement and the potential abuse in violation of the privacy of the citizen should be discussed and solved.

9 CONSEQUENCES OF THE GAP OF A NATIONAL IT-SECURITY

- Competition disadvantages: Missing, retarded or too expensive foreign certifications might keep away Austrian products of the information sector from some markets, like North-America or the European Community.
- Restrictions in the evolvement of high-level telematic services: Missed or non-trustworthy security mechanisms may restrict new telematic-services, like home-banking, ... or reduce the acceptance of this services.
- Restricted legal protection: Unsuitable security activities and regulations may result in unrecovered abuse of information techniques or in a lack of law enforcement against abuse of information technique. This can endanger some central social and political achievements of the Austrian society, like privacy, freedom of speech, good protective labour legislation, consumer protection, guarantee-rights by information services.
- Eclusion from important international developments: The absence of Austria in the definition phase of security policy may reduce the ability of Austrian research institutes to reach the latest informations in the area of IT-security.

10 ACTIVITIES TOWARDS A NATIONAL SECURITY-POLICY

1) Definition of the job profile "commissioner of data protection" and organization of an equivalent graduate or post-graduate study. This study should include informatical and non-informatical areas, like social responsibility of data processing.
2) Reduction of administrative obligations, like registration of data processing systems, if an organisation has good internal security provisions.

3) Promotion of information products and services (hardware and software) with integrated technical security functions.
4) Intensifying of basic research to define standard functions for telematic-services, like secure mail or classifying of information.
5) Foundation of an advisory board for all tasks, questions and activites in the practical translation of security-policy-provisions.

All this propostions are conforming with the intentions of the European Community and are part of the new directive of data-protection of the EC.

11 PERSONAL ANNOTATION:

There are common concerns of commercial and national security. But there is also a tremendous conflict between both of these types of security requirements. National institutions, like national police may have an increasing demand to protect their own national and international information databases (e.g. Schengen information system), but also to get better and full access to the protected commercial informations systems, e.g. in the banking sector.

Good and effective security activities, like data encryption, might contradict the goal of fighting against organised crime. Mechanisms of authorised interception of commercial information traffic for law enforcement, may on the other hand restrict private and personal rights in an inadmissible manner.

This situation requires an objective and non-governmental mechanism to balance this different demands of a national security policy.

In my opinion the best way is to find general legistic regulation and an organisation for the operative realization of this task.

12 REFERENCES

Amt für amtliche Veröffentlichungen der EG [ed.] (1991) Kriterien für die Bewertung der Sicherheit von Systemen der Informationstechnik. Luxembourg. [ITSEC]

Amt für amtliche Veröffentlichungen der EG [ed.] (1994) Information Technology Security Evaluation Manual, *Provisional Harmonized Methodology*. Luxembourg. [ITSEM]

Beschluß des Rates vom 31. März 1992 auf dem Gebiet der Sicherheit von Informationssystemen (92/242/EWG; ABl. L123/19, 08.05.92). Bruessels. [EUSEC]

BSI Bundesamt für Sicherheit in der Informationstechnik [ed.] (1992) IT-Sicherheitshandbuch, *Handbuch für die sicherer Anwendung der Informationstechnik*, Bonn. [ITSHB]

Bundeskanzleramt (1993) Datenschutzbericht der Datenschutzkommission. Bundeskanzleramt, Wien. [DSK93]

Common Criteria Editorial Board (1994) Common Criteria Unclassified Version V0.2, *Information Technology Security Evaluation Common Criteria*. CD-ROM, Bruessels. [CC94]

DG XIII: Telekommunications, Information Market and Exploitation of Research [ed.] (1994) Green Paper on the Security of Information Systems. Bruessels. [GREEN94]

Dohr, W., Weiss, E. M. et.al. (1988) Datenschutzgesetz, *in der ab 1. März 1988 geltenden Fassung (actual issue: http://www.ad.or.at/text/gesetze.htm)*. Manz, Wien. [öDSG]

Europäisches Parlament (1995) Gemeinsamer Standpunkt des Rates vom xxxxx im Hinblick auf den Erlaß der Richtlinie 95/xxx/EG des Europäischen Parlaments und des Rates zum

Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten und zum freien Datenverkehr. Bruessels. [EUDSR]

Kommission der Europäischen Gemeinschaft (1994) Geänderter Vorschlag für eine Richtlinie des Europäischen Parlaments und des Rates zum Schutz personenbezogener Daten und der Privatsphäre in digitalen Telekommunikationsnetzen, *insbesondere im diensteintegrierenden digitalen Telekommunikations und digitalen Mobilfunknetzen (gemäß Artikel 189 A, Absatz 2 des EG-Vertrages von der Kommission vorgelegt), KOM(94) 128 endg.-COD 288*. Bruessels. [ISDN]

Simone Fischer-Hübner (1994) Ein formales Datenschutzmodell:, in *Sicherheit in Informationssystemen, Proceedings der Fachtagung SIS `94 Universität Zürich-Irchel, Institut für Informatik 10.-11. März 1994* (ed. Prof. Dr. Kurt Bauknecht, Dr. Stephanie Teufel). Zürich. [SIS-FI]

U.S. Department of Commerce National Technical Information Service (1985) Department of Defense trusted Computer System Evaluation Criteria *(Orange Book)*. DoD, Washington DC. [TCSEC]

Vranitzky, F. (1994) Weichenstellung für ein digitales Österreich, *Rede von Bundeskanzler Dr. Franz Vranitzky bei den Alpbacher Technologiegespraechen.* Alpbach. [VRAN]

13 BIOGRAPHY

Hans G. Zeger received both the M.Sc. and the Ph.D. degrees from the University of Vienna in 1980 and 1982. Currently he hold the position of the chairman of the ARGE DATEN - Austrian Society of dataprotection and privacy.

Prior he is working in the Software Engineering Aera in same major Austrian computing centers (1983-1987).

Implementing a fulltext information and retrieval system for a leading Austrian pharmaceutical company. In this area I was responsible for the design of the fulltext databases, for the inhouse-network and the wide area access via the public packet switching network (1988 - 1990).

Now he is working in the own service organisation of the ARGE DATEN as Consultant for security evaluation, data protection and risk analyses.

He is also lecture at the Universities of Vienna, Linz and Innsbruck with the special fields data-protection, privacy and telecommunication.