

#### **NOTE OF THE COMPONENT COORDINATOR REGARDING THE ACCOMPLISHMENT OF THIS ACTIVITY**

To work in the public sector in general and so in the DSI as well, is neither very attractive for IT specialists nor is the payment an incentive, compared to what opportunities IT specialists have in the emerging private sector. This factor is common between the DSI and a lot of public institutions in Germany.

So it is not surprising that besides the director (who has a technical background and experience), the next technician in the DSI is a part time student. He is well qualified, but available only part of the time.

Taking this into account, it is to accredit that the DSI staff members were able to set up a fairly comprehensive audit manual (even if that is based largely on the British original).

Even though the DSI receives complaints from external auditors about the comprehensiveness of the manual, this is a qualified document and not “just bureaucratic rules and regulations”, but a helpful introduction on how to conduct audits.

While we were not able to receive a control report based on the described manual, we can only encourage the DSI to stay with this manual and to enhance this to success.

Roman Maczkowsky

COMPONENT 3: IMPROVEMENT OF DSI CAPACITY IN RESPECT OF INSPECTIONS  
OF PERSONAL DATA PROCESSING SYSTEMS

ACTIVITY 3.1: PREPARATION OF A MANUAL ON AUDITING THE SECURITY OF  
PERSONAL DATA PROCESSING SYSTEMS

**MANUAL**  
**ON AUDITING THE SECURITY**  
**OF PERSONAL DATA PROCESSING SYSTEMS**

FOCUSING ON  
EUROPEAN UNION MEMBER STATES PRACTICE  
AND TAKING INTO ACCOUNT  
SPECIFIC REQUIREMENTS AND CIRCUMSTANCES IN LATVIA

BY

ROMAN MACZKOWSKY

JAN MÖLLER

# CONTENT

<b>1. INTRODUCTION</b>	<b>4</b>
<b>2. LEGAL REQUIREMENTS REGARDING THE SECURITY OF PERSONAL DATA</b>	<b>5</b>
1.1 PROVISIONS OF DIRECTIVE 95/46/EC	5
1.1.1 ART. 16 DIRECTIVE 95/46/EC CONFIDENTIALITY OF PROCESSING	6
1.1.2 ART. 17 DIRECTIVE 95/46/EC SECURITY OF PROCESSING	8
ART 17 (1) DIRECTIVE 95/46/EC TECHNICAL AND ORGANISATIONAL MEASURES	8
ART 17 (2) AND (3) DIRECTIVE 95/46/EC PERSONAL DATA PROCESSING BY ORDER	10
ART 17 (4) DIRECTIVE 95/46/EC FORMAL REQUIREMENTS	11
1.2 NATIONAL LEGISLATION IMPLEMENTING THE REQUIREMENTS OF DIRECTIVE 95/46/EC	12
1.2.1 INVENTORY OF NATIONAL LEGAL PROVISIONS	12
LATVIAN PERSONAL DATA PROTECTION LAW	12
REGULATIONS	12
SPECIAL AREA PROVISIONS	13
1.2.2 WAY OF IMPLEMENTATION	13
DETAILED LEGISLATION	13
GENERAL CLAUSE AND BEST PRACTICE GUIDES	14
1.2.3 PROBLEMS RELATING TO LEGISLATION	14
SCOPE OF IMPLEMENTATION	14
UPDATING IT SECURITY REQUIREMENTS	14
<b>3. TECHNICAL REQUIREMENTS REGARDING THE SECURITY OF PERSONAL DATA</b>	<b>15</b>
1.3 INVENTORY OF EXISTING TECHNICAL DOCUMENTS	15
1.3.1 REGULATIONS:	15
1.3.2 DESCRIPTION	15
[INTENDED] COMPARISON WITH REAL CASES (CONTROLS)	15
ANALYSING THE EXISTING DATA PROTECTION AUDIT MANUAL	15
1.3.3 EVALUATION	16
INTENDED AUDIENCE	16
STANDARDS CONFORMITY	16
DEALING WITH IT-SECURITY	16
TECHNICAL IT-SECURITY MEASURES	16
IDENTIFYING CONFLICTING FIELDS OF DATA PROTECTION AND IT-SECURITY	16
1.4 FURTHER REQUIREMENTS	17
EXAMPLE: "CREDENTIALS"	17
THE IMPORTANCE OF APPROPRIATE RISK ANALYSES	18
1.4.2 CAPABILITIES BASED ATTACK TREE RISK ANALYSIS METHODOLOGY	18
TOOLS FOR RISK ANALYSIS	19
1.4.3 EXAMPLES FOR IT-SECURITY RECOMMENDATIONS	19
ABSTRACT	19
GETTING THE OVERVIEW	19
THREAT MODELING AND RISK ANALYSIS	20
THE AUDIT-DATA TRAIL PROBLEM	20
USER TRACKING TECHNIQUES	21
REQUIREMENTS FOR BACKUPS AND BACKUP STORAGE	21
CRYPTOGRAPHIC TECHNOLOGIES AND ALGORITHMS	22

BIOMETRIC DATA	23
SECURE TERMINAL EQUIPMENT (WORKPLACE PC)	24
WIRELESS LAN SECURITY	25
WIRELESS DATA TRANSMISSIONS VIA BLUETOOTH AND IRDA	26
<b>4. RECOMMENDATIONS</b>	<b>27</b>
<b>5. ANNEXES</b>	<b>28</b>
1.5 LEGAL PROVISIONS REGARDING THE SECURITY OF PERSONAL DATA	28
1.5.1 DIRECTIVE 95/46/EC	28
ARTICLE 16 CONFIDENTIALITY OF PROCESSING	28
ARTICLE 17 SECURITY OF PROCESSING	28
RECITAL (46)	28
1.5.2 CONVENTION FOR THE PROTECTION OF INDIVIDUALS WITH REGARD TO AUTOMATIC PROCESSING OF PERSONAL DATA (ETS No. 108)	29
ARTICLE 7 DATA SECURITY	29
1.5.3 LATVIAN PERSONAL DATA PROTECTION LAW	30
SECTION 26	30
SECTION 27	30
1.5.4 LATVIAN CABINET OF MINISTERS REGULATIONS No 40 (OF 30.01.2001)	31
OBLIGATORY TECHNICAL AND ORGANIZATIONAL REQUIREMENTS FOR PROTECTION OF PERSONAL DATA PROCESSING SYSTEMS	31
1.5.5 GERMAN FEDERAL DATA PROTECTION ACT	33
SECTION 5 CONFIDENTIALITY	33
SECTION 9 TECHNICAL AND ORGANIZATIONAL MEASURES	33
SECTION 11 COLLECTION, PROCESSING OR USE OF PERSONAL DATA BY AN AGENT	33
ANNEX (TO THE FIRST SENTENCE OF SECTION 9 OF THIS ACT)	33
1.6 TECHNICAL DOCUMENTS REGARDING THE SECURITY OF PERSONAL DATA PROCESSING	35
1.6.1 DSI DATA PROTECTION MANUAL	35
1.6.2 PROTECTION REQUIREMENT CATEGORIES	36
1.6.3 CAPABILITIES-BASED ATTACK TREE ANALYSIS	37
THREE KEY BENEFITS OF ATTACK TREE ANALYSIS	40
1.6.4 COMMENT ON THE "MANUAL OF AUDIT OF DATA PROCESSING SYSTEMS" BY STE DR. T. PROBST	42

## 1. INTRODUCTION

The Activity 3.1 is entitled: “Preparation of a manual on auditing the security of personal data processing systems”. The following tasks were planned to be carried out in close co-operation between the Member States Short Term Experts and Latvian Experts:

Analysing the current practice in Latvia and comparing it with the practice in Germany

Develop a practical handbook / manual on auditing the security of personal data processing systems.

While we tried to evaluate the current practice of auditing the security of personal data processing systems, the DSI presented us a new handbook called “Data Protection Manual” and promised access to the files of a control case with technical emphasis for analysis. This promise was postponed several times despite repeated requests for access and no document was made available until the end of this activity.

Therefore we were not able to compare the Latvian practise in this field, but could discuss and present good EU Member States practises on auditing the security of personal data processing systems.

The analysis of the existing data protection manual was a positive surprise, so we decided to not reinvent the wheel, but to analyse the existing handbook and make proposals for improvement. The analysis of the DSI data protection manual can also be found as a summary in Section 3 and more detailed as the report of STE Dr. Thomas Probst in the Annex.

In reaction to a first discussion about the manual, the Project Leader CC asked us to help in the development of a more in-depth technical part. Examples of advices towards the requested items can be found in section 3 of this document.

The analysis of the referenced national laws and regulations in the audit manual revealed room for improvement in the national legislation. The legal analysis therefore focuses on the requirements regarding the security of data processing systems of Directive 95/46/EC and their practical and effective implementation into national law.

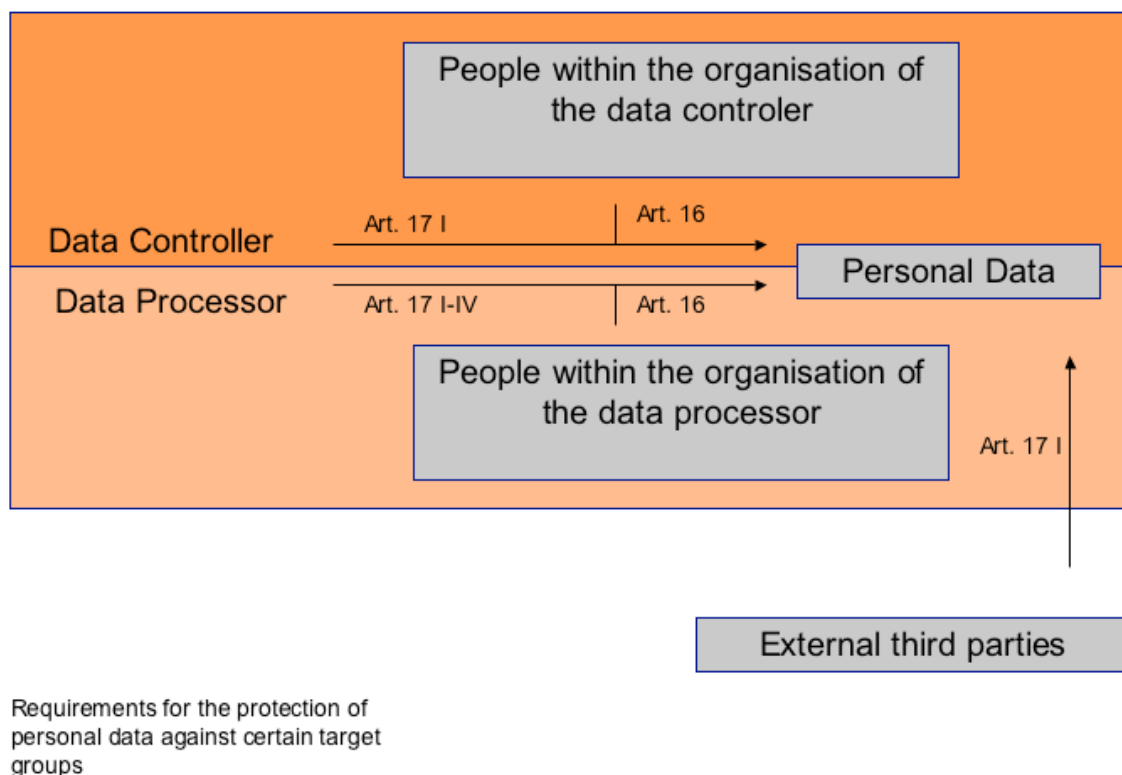
## 2. LEGAL REQUIREMENTS REGARDING THE SECURITY OF PERSONAL DATA

### 1.1 PROVISIONS OF DIRECTIVE 95/46/EC

Art. 16 and 17 Directive 95/46/EC establish regulations on the confidentiality and security of personal data. They are setting a minimum standard of technical and organisational security of personal data that has to be implemented in the national data protection legislation. Therefore the knowledge and European law compliant interpretation of these provisions is the legal basis for the proper application of national provisions implementing the Directive requirements concerning the security of personal data.

The provisions address different *target groups* and different *processing situations*. The common starting point is the *risks* that actually might occur in the course of the processing of personal data.

Risks can emerge from different participants involved in the processing. Therefore the provisions address obligations of the data controller and persons acting within its organisation (employees, etc.), potentially involved data processors which are processing personal data by order of the data controller and persons within its organisation and other people who are external from data controller and data processor. The obligations include the implementation of technical and organisational measures as well as the fulfilment of material legal requirements.



The persons acting within the organisation of the data controller are targeted by the confidentiality requirement found in Art. 16 Directive 95/46/EC.

More complicated questions of responsibility for and control of data processing arise if the data controller is using other parties outside of its own organisational power to fulfil contractual or other obligations that require personal data processing. To sustain the level of data protection for these personal data handed over into a data processor's sphere of

influence, material requirements have to be met as a precondition for the legality of such data processing by order. Therefore – besides the applicability of Art. 16 to persons acting in behalf of the data processor – the Directive 95/46/EC statutes material (Art. 17 (2) – (3)) permission requirements for data processing in behalf of the data processor. Further formal exigencies regarding contracts or legal acts on data processing by order can be found in Art. 17 (4).

Finally Art. 17 (1) requires technical and organisational measures protecting personal data from being processed by external persons who are not part of the data controller and the data processor. Formal requirements regarding the documentation of these measures are laid down in Art. 17 (4).

The abovementioned legal provisions include a number of terms that are defined by the Directive itself or in different contexts of the Directive's provisions. The following table helps to identify terms legally defined and to find the definition:

<b>TABLE OF LEGAL DEFINITIONS</b>
For definition of "controller" see Art. 2 (d) Directive 95/46/EC
For definition of "processor" see Art. 2 (e) Directive 95/46/EC
For definition of "personal data" see Art. 2 (a) Directive 95/46/EC
For definition of "processing of personal data" see Art. 2 (b) Directive 95/46/EC
For definition of "destruction" compare Art. 2 (b) Directive 95/46/EC
For definition of "alteration" compare Art. 2 (b) Directive 95/46/EC
For definition of "disclosure" compare Art. 2 (b) and Art. 2 (g) Directive 95/46/EC
For definition of "access" compare Art. 2 (b) Directive 95/46/EC the definition of "otherwise making available"
For definition of "forms of processing" compare Art. 2 (b) Directive 95/46/EC
For definition of "nature of data" compare Art. 8 (1) Directive 95/46/EC
For definition of "processing on the behalf of the controller" compare Art. 2 (e) Directive 95/46/EC
For definition of "processing by way of a processor" compare Art. 2 (e) Directive 95/46/EC

#### 1.1.1 ART. 16 DIRECTIVE 95/46/EC CONFIDENTIALITY OF PROCESSING

According to the heading Art. 16 Directive 95/46/EC provides for the confidentiality of the processing of personal data by those persons who have access to it at the data controller as well as at the data processor. But the scope of the provision is broader than "confidentiality" as everybody who "acts under the authority" of the data controller and the data processor is bound to the instructions of the data controller concerning the processing of the personal data. The deviation between heading and content of this provision results from the change

of the provision in the changed proposal of the EU-Commission. Earlier versions were aiming not on all forms of processing but just the disclosure of personal data. The existing provision is also violated i.e. if personal data is altered or destroyed against the instruction of the data controller.

That example shows that the scale for judging a breach of confidentiality according to the Directive 95/46/EC is not compliance of data processing with the applicable data protection regulations but conformity with the instructions of the data controller.<sup>1</sup> This complies with the sole responsibility of the data controller for the data processing. Therefore according to Art. 16 Directive 95/46/EC there is no obligation of data processors to judge the legal compliance of instructions of the data controller. Nevertheless even if obviously illegal processing by a data processor that is in line with the instruction of the data controller cannot be considered a breach of confidentiality according to the Directive 95/46/EC it still can be a deliberate act of supporting possibly criminal behaviour of the data controller. Moreover national legislation can add to the protection standard by implementing a notification obligation for the data processor if he realizes non law-compliant processing by order.

The respective implementing provisions in Germany add additional requirements to the confidentiality rule. § 5 FDPA (GERMAN: BDSG) in Germany includes a two level model that extends the obligations of the data controller to follow the data protection legislation as a personal obligation to each person acting under his authority.<sup>2</sup> As a second level the extent of personal data processing that is allowed for certain persons is determined by the instructions (tasks, contract etc.) with the data controller. This implementation obviously puts a higher standard to the persons actually involved in personal data processing. Respectively § 5 FDPA (GERMAN: BDSG) also requires an “act of commitment” of the persons by the non public data controller to inform them clearly about their obligations and risks of non-compliance.

All persons accessing personal data “acting under the authority” of the data controller, the data processor or further data processors are within the scope of the provision. This includes employees, people working freelance and other auxiliary persons<sup>3</sup> contractually or otherwise bound to data controller and data processors as well as the representatives of the data processors and the data processor itself even if it is already bound by a similar obligation in Art 17 (3) 1.<sup>4</sup> Additionally further data processors that work on the behalf of the data processor (cascades of data processors) are bound to the instructions. Therefore respective contractual provisions between all data processors involved are advisable (See also commentary to Art. 17) if data processing is distributed to cascades of data processors.

An exception from the obligation to follow the instructions of the data controller was included in the changed proposal of the EU-Commission. According to this exception the group of obliged persons (see above) may process personal data if there is a legal obligation forcing them personally (not just the data controller) to do so, i.e. to witness in court, to avert imminent crimes.<sup>5</sup> Sanctions for non-compliance are not mandatory in the Directive 95/46/EC but can be implemented in national legislations of the Member States<sup>6</sup>

German legislation considers certain constellations of breaches of § 5 FDPA (German: BDSG) as an administrative offence according to § 43 (2) FDPA<sup>7</sup> or a criminal offence according to § 203 German Criminal Code (StGB)<sup>8</sup>.

---

<sup>1</sup> Dammann/Simitis, EU-Datenschutzrichtlinie: Kommentar, 1. ed., Baden Baden 1997, Art. 16 , 5.

<sup>2</sup> Walz in Simitis, Kommentar zum BDSG, § 5, 5, 21, 23.

<sup>3</sup> Dammann/Simitis, EG-Datenschutzrichtlinie: Kommentar, 1. ed., Baden Baden 1997, Art. 16, 3.

<sup>4</sup> Dammann/Simitis, EG-Datenschutzrichtlinie: Kommentar, 1. ed., Baden Baden 1997, Art. 16, 4.

<sup>5</sup> Reasoning of the changed proposal, see Dammann/Simitis, EG-Datenschutzrichtlinie: Kommentar, 1. ed., Baden Baden 1997, Art. 16, 7.

<sup>6</sup> Ehmann / Helfrich, EG-Datenschutzrichtlinie: Kurzkomentar, 1. ed., Cologne 1999, Art. 16, 8.

<sup>7</sup> Walz in Simitis, Kommentar zum BDSG, § 5, 36 ff.

## 1.1.2 ART. 17 DIRECTIVE 95/46/EC SECURITY OF PROCESSING

## ART 17 (1) DIRECTIVE 95/46/EC TECHNICAL AND ORGANISATIONAL MEASURES

Art. 17 (1) Directive 95/46/EC requires the Member States to foresee an obligation for the data controllers in their national legislation to implement “appropriate technical and organisational measures” against certain accidental, certain accidental or unlawful and all other forms of unlawful processings of personal data. Regarding the *state of the art* and the *cost of the implementation* these measures have to offer a *level of protection appropriate to the risks of processing* and the *nature of data*.

The obligation of the data controller to take “appropriate technical and organisational measures” to protect personal data from certain events that could endanger the privacy of the data subject is a fairly broad and general term that is substantiated with a catalogue of practically relevant risk situations whose realization should be avoided by the measures.

It includes the accidental or unlawful destruction or accidental loss, alteration, unauthorized disclosure or access, in particular where the processing involves the transmission of data over a network, and *against all other unlawful forms of processing*. This means that the actual cause of an unlawful processing is not relevant.<sup>9</sup> It could be a deliberate act as well as an accidental event. Art 17 Directive 95/46/EC intends to avoid unlawful processings and to reduce their likeliness. Measures therefore have to be targeted to that goal according to the respective risk (principle of risk minimization<sup>10</sup>).

Examples of measures can include access control to premises and computer systems, measures against fire, flooding or natural powers, encryption, system surveillance and monitoring of unusual system activity.<sup>11</sup> Further examples can be found in the reasoning of Art.18 Directive 95/46/EC of the original proposal of the EU-Commission.

*The level of abstraction how technical and organisational measures are implemented is left to the Member States as long as an adequate protection level is kept.* The German legislation implements Art. 17 (1) Directive 95/46/EC in § 9 FDPA. To substantiate the meaning of technical and organisational measures an annex to § 9 (1) FDPA (GERMAN: BDSG) was added to the law that gives a structure of which types of measures are meant. This annex is included in 5.1.3 as an example and highly recommended for reading at this point.

A rapidly developing technical sector makes the successful avoidance of unlawful processings a difficult to reach target that renders an inflexible and formal canon of IT security measures worthless. Actual measures have to be oriented on existing risks. That is why a thorough risk analysis concerning the processing situation has to be carried out and a following risk assessment should enable the determination which measures are appropriate in the particular situation.<sup>12</sup> Two conclusions of a risk assessment for example could be that personal data processing systems used in regions with regular flooding should be in respectively reinforced premises (what might not be necessary elsewhere) or that systems without exchange of data with other networks do need less or different protection against viruses and other malicious software than systems connected to the internet.

After risk analysis and risk assessment a balancing of interests has to take place. Recital 46 specifies that the appropriate measures should account the *state of the art* and the *costs of their implementation* in relation to the *risks inherent in the processing* and the *nature of the data* to be protected. The term “*state of the art*” has to be determined according to the

---

<sup>8</sup> Walz in Simitis, Kommentar zum BDSG, § 5, 39.

<sup>9</sup> Dammann/Simitis, EG-Datenschutzrichtlinie: Kommentar, 1. ed., Baden Baden 1997, Art. 17, 3.

<sup>10</sup> Dammann/Simitis, EG-Datenschutzrichtlinie: Kommentar, 1. ed., Baden Baden 1997, Art. 17, 7.

<sup>11</sup> Ehmann/Helfrich, EG-Datenschutzrichtlinie: Kurzkomentar, 1. ed., Cologne 1999, Art. 17, 3.

<sup>12</sup> For comprehensive information on risk analysis and assessment see Münch, Technisch-organisatorischer Datenschutz – Leitfaden für Praktiker, 1. ed, Frechen 2003, p. 93.

actually available technical possibilities for usage at the time of assessment. It is not limiting or excluding any measures as long as they are offering an effective protection level. It also includes a regular update of such measures to maintain the protection level in the future. This is of special importance as developments in technology are advancing very rapidly and can render old measures without effect after only a short period of time. The implementation and regular update of modern and effective technical and organisational measures can be expensive. Therefore it was discussed<sup>13</sup> if the costs of implementation have to be considered as a factor in the balancing of interest. The final wording requires them to be included but not as plain absolute numbers. The costs have to be considered in relation to the nature of the data and the inherent risk of their processing. This means that i.e. the processing of sensitive data with high risk for the data subject's right to informational self-determination justifies even high costs for technical and organisational measures while for personal data whose unlawful processing would be less invasive to data subject's privacy the same technical and organisational measures could be out of relation. The structure of the balancing process and the arguments that has to be taken into account is set in the Directive The actual method of risk analysis and risk assessment as well as the fitting measures itself has to be determined by IT security and data protection experts in the respective situation.<sup>14</sup>

As a result of the processes of risk analysis, risk assessment and balancing of interests of data controller and data subject the *appropriate* technical and organisational measures for a particular personal data processing situation should be determined. The group of measures should be laid down and coordinated in a protection concept that offers a basis for the actual implementation of the measures and a documentation of data controller's activities of technical and organisational data protection.

Protection concepts are usually aiming at the measures to be taken at the time of processing but recital 46 states that technical and organisational measures have to be taken also *at the time of the design of the processing system* as well as *at the time of the processing*. In best case measures taken at both times are integrated in one protection concept. This requires that protection concepts are drawn up already before processing systems are developed or bought and that these systems are evaluated regarding implemented and still necessary security measures. The EU-Commission considers measures already taken in the design of processing systems very important for the development of future personal data processing systems.

The first report on the implementation of the Directive 95/46/EC was released on 16<sup>th</sup> May 2003. Section 4.3 on the „Promotion and encouragement of Privacy Enhancing Technologies“ (PET) contains further information on what can be considered appropriate technical and organisational measures taken at the time of design of the processing system:

„Promotion and encouragement of Privacy Enhancing Technologies

The idea of Privacy Enhancing Technologies is to design information and communication systems and technologies in a way that minimises the collection and considers that the use of appropriate technological measures is an essential complement to legal means and should be an integral part in any efforts to achieve a sufficient level of privacy protection.

Technological products should be in all cases developed in compliance with the applicable data protection rules. But being in compliance is only the first step. The aim should be to have products that are not only privacy-compliant and privacy-friendly but if possible also privacy-enhancing<sup>26</sup>.

---

<sup>13</sup> Ehmann/Helfrich, EG-Datenschutzrichtlinie: Kurzkomentar, 1. ed., Cologne 1999, Art. 17, 6.

<sup>14</sup> Further information for the current state of the art can be found in the section “Technical requirements” below 3.

During the discussions on PETs at the Commission's 2002 conference on the implementation of the Directive, it was pointed out that the use of certain technical tools makes it impossible for controllers to comply with the law. ...

Footnote 26 of the report:

See in this sense the conclusions of the document WP 37 of the Article 29 Working Party, November 2000: "*Privacy on the Internet - An integrated EU Approach to On-line Data Protection*". Privacy compliant products are products developed in full compliance with the Directive, privacy-friendly products go one step further by introducing some elements that make the privacy aspects more easily accessible to the users like for instance by providing very user-friendly information to the data subject or very easy ways of exercising their rights. Privacy-enhancing products are those that have been designed in a way that aims at accomplishing the largest possible use of truly anonymous data. [http://europa.eu.int/comm/justice\\_home/fsj/privacy/docs/wpdocs/2000/wp37en.pdf](http://europa.eu.int/comm/justice_home/fsj/privacy/docs/wpdocs/2000/wp37en.pdf)

#### ART 17 (2) AND (3) DIRECTIVE 95/46/EC PERSONAL DATA PROCESSING BY ORDER

Art. 17 (2) and (3) Directive 95/46/EC require the data controller to take certain protection measures for the case that it intends to use a data processor external to its own organisation for its personal data processing. By this means the protection level of personal data shall be maintained even in this practically very relevant processing situation.

The data processor is a legal or natural person who processes personal data on behalf of a data controller but is not an employee of a data controller who processes such data in the course of his employment. According to Art. 2 f Directive 95/46/EC he is not considered a third party but is treated similar to an employee of the data controller.<sup>15</sup> Problems might occur in cases where a data controller uses freelancers or self-employed persons to process personal data. For the decision if these are considered still part of the data controller (then bound by provisions implementing Art. 16 Directive 95/46/EC) or are considered to be data processors (then the following requirements have to be fulfilled) it has to be looked to their contractual binding to the data controller and their freedom to exercise own discretion not just regarding personal data processing.

National legislation has to oblige the data controller to choose a data processor who guarantees appropriate protection measures (Art. 17 (2) Directive 95/46/EC, necessity to responsible choice<sup>16</sup>). This can be checked according to a protection or security concept of technical and organisational measures according to Art. 17 (1) Directive 95/46/EC. The concept can be proposed and its implementation has to be guaranteed by the data processor. The responsibility to control if the proposed measures are *appropriate* stays with the data controller. Moreover the data controller also stays responsible for the control that the concept is actually implemented and updated and that the measures are effective. The data controller can use official experts and tested and / or certified technology to fulfil its duties.

Personal data processing has to be based on a contractual relationship or a legal act binding the data processor to the data controller (Art. 17 (3) Directive 95/46/EC). Personal data processing based on legal acts might especially happen in the public sector. If data controller and data processor cannot reach agreement according to appropriate measures or other substantial parts of the contract that might affect the privacy of the data subject the data controller has to finish the contract and to cease personal data processing by this data processor.

The contract has to stipulate that the data processor shall act *only on instructions* from the controller. This is to clarify that the data controller may not delegate the execution of

<sup>15</sup> Dammann/Simitis, EG-Datenschutzrichtlinie: Kommentar, 1. ed., Baden Baden 1997, Art. 17, 6.

<sup>16</sup> Dammann/Simitis, EG-Datenschutzrichtlinie: Kommentar, 1. ed., Baden Baden 1997, Art. 17, 10.

discretion to the data processor if or how personal data is processed and no matter if this personal data was transferred from the data controller, collected on his behalf or created newly.<sup>17</sup> The full responsibility for the personal data processing stays with the data controller corresponding with the sole right to decide about the processing. Therefore a valid legal binding of the data processor to the instructions of the data controller is necessary. The aforementioned distribution of responsibilities also leads to the situation that the rights of the data subject have to be asserted against the data controller even if the actual processing is executed by a data processor. Also registration and other obligations are bound to the data controller.

Especially with the rising numbers of outsourcing cases it is important to distinguish the position of a data processor whose task has a helping character from the situation that another data controller executes certain data operation on his own and exercises his own discretion in fulfilling this task for the data controller. These cases of *transfer of functions*<sup>18</sup> are not privileged as a data processing by order and have to be considered as a normal transfer of data between data controllers which requires a legal permission (consent or legal provision).

The contract between data controller and data processor must also include an obligation of the data processor to implement the appropriate technical and organisational measures according to Art. 17 (1) Directive 95/46/EC. As mentioned the judgement of appropriateness is to be done by the data controller. The obligations set out in (1) have to be implemented, as defined by the law of the Member State in which the processor is established. Therefore data processors that work for data controllers in different Member States do not need to offer different implementations or types of technical or organisational measures. If different levels of protection regarding technical and organisational measures in different Member States occur this could lead to distortions in competition of data processors and opens a possibility for data controllers to lower the standards.

#### ART 17 (4) DIRECTIVE 95/46/EC FORMAL REQUIREMENTS

Art. 17 (4) Directive 95/46/EC includes formal requirements for the processing contract or legal act. For the purposes of keeping proof, the parts of the contract or the legal act relating to data protection and the requirements relating to the measures referred to Art. 17 (1) Directive 95/46/EC shall be in writing or in another equivalent form. This formal requirement is clarify the responsibilities of the parties. The goal is prevention. It is not considered to be necessary for the validity of the contract. The written form is kept if a contract is signed by the parties. The handwritten signature has to cover all parts relevant for data protection and the appropriate technical organisational measures according to Art. 17 (1) Directive 95/46/EC<sup>19</sup> As an example there should be a clear description of the processing instructions, rules of transfer, measures of quality management concerning the personal data and their legality of processing.

An equivalent form to “in writing” is acceptable if it has a binding character and protects the originality the content in a permanent manner.<sup>20</sup>

---

<sup>17</sup> Dammann/Simitis, EG-Datenschutzrichtlinie: Kommentar, 1. ed., Baden Baden 1997, Art. 17, 13.

<sup>18</sup> Walz in: Simitis, Kommentar zum Bundesdatenschutz, 5. ed, Baden Baden 2003, § 11, 18.

<sup>19</sup> Dammann/Simitis, EG-Datenschutzrichtlinie: Kommentar, 1. ed., Baden Baden 1997, Art. 17, 15.

<sup>20</sup> Dammann/Simitis, EG-Datenschutzrichtlinie: Kommentar, 1. ed., Baden Baden 1997, Art. 17, 15, Ehmann/Helfrich, EG-Datenschutzrichtlinie: Kurzkomentar, 1. ed., Cologne 1999, Art. 17, 13f.

## 1.2 NATIONAL LEGISLATION IMPLEMENTING THE REQUIREMENTS OF DIRECTIVE 95/46/EC

The requirements of the Directive 95/46/EC outlined above have to be implemented by the national legislation. The Latvian legislator intends to implement these requirements with the following laws and regulations.

### 1.2.1 INVENTORY OF NATIONAL LEGAL PROVISIONS<sup>21</sup>

The basic provisions of implementation are located in the Latvian Data Protection Law.

#### LATVIAN PERSONAL DATA PROTECTION LAW

The Latvian Personal Data Protection Law is applicable to both the public and the non-public sector. The IT security requirements are therefore applicable to both companies and public institutions if not otherwise stated.

#### SECTION 25

Section 25 of this law requires the necessary technical and organisational measures for the protection of personal data according to Art. 17 Dir. 95/46/EC to be taken to prevent their illegal processing. The technical and organisational measures chosen in the respective cases have to be declared in the application for registration of a personal data processing system (Section 22 No. 16) although they do not become part of the public register (Section 24 No. 1).

Paragraph 2 of this section includes more detailed information of the responsibility in cases of data processing by order and regulates the power to decide about personal data processing.

#### SECTION 26

Sections 26 leaves the determination of the mandatory technical and organisational requirements to the Cabinet. The more detailed determination is done in the Regulation(s) 40 (and 106) and might be done in further regulations on state data information systems as described below.

Moreover it requires government and local government institutions (a big part of the public sector) institutions to a yearly internal audit. The results including the risk analysis and measures taken have to be submitted to the DSI that enables DSI to cross check general IT security situation in this field. The careful evaluation of audit reports makes sense but appropriate consultancy or control of such institutions and their security concepts requires a considerably amount of time of qualified technical personnel.

#### SECTION 27

Section 27 paragraph 1 implements Art. 16 Dir. 95/46/EC concerning the confidentiality requirement of the employees of the data controllers (system controller according to Section 2 No. 9) and processors (personal data operator according to Section 2 No.6). Paragraph 2 includes a recording requirement for the commitments according to paragraph 1 that enable DSI to control and enforce this regulation. Paragraph 3 includes the basic principle of data processing by order that the processor shall comply with the instructions of the system controller.

#### REGULATIONS

Section 26 refers to the determination of the mandatory technical and organisational requirements. Therefore<sup>22</sup> Regulation No. 40 of the Cabinet of Ministers of January 30<sup>th</sup>, 2001 was implemented by the Latvian government.

---

<sup>21</sup> As far as made available to the author in English language.

<sup>22</sup> See the reference to Section (here translated "Article") 26 of the Personal Data Protection Law in Reg. 40.

## REG. NO. 40

The Regulation No. 40 references Regulation No. 106 of March 21<sup>st</sup>, 2000 which meanwhile is outdated. A replacement or prolongation has not been installed by the time of examination. Therefore the reference in No. 2 of Reg. 40 concerning the general provisions for protection of personal data processing systems is not implementing such measures in the legal concept of IT security anymore. This opens a protection hole in the mandatory technical and organisational requirements. Probably the “state of the art” as mentioned in Art. 17 Dir. 95/46/EC will not be achieved in certain cases if the measures according to Reg. 106 are simply left out, as they are not mandatory anymore.

## REG. NO. 106

Reg. 106 consist of a long list of IT security measures that are appropriate in certain processing situations. Reg. 40 and Reg. 106 are respectively were (at the time it was in force) applicable to the private sector as well as to the public sector.<sup>23</sup>

## SPECIAL AREA PROVISIONS

Besides this general provisions concerning IT security special regulations can be overriding.

## STATE INFORMATION SYSTEMS

The relation of the Personal Data protection Law to the Cabinet of Ministers Regulations on State Information systems<sup>24</sup> that initially were introduced to us as the successor of Reg. 106 is not yet clear. The drafts of these regulations that were not in force at the time of examination were kindly made available to the project. These regulations expressively refer to Section 4 of the Law on State information systems. State information Systems are according to Art. 1 No. 1 Sate Information Systems Law a structured assemblage of information technologies and data bases, to enable the stimulation, creation, collection, recording, processing, use and destruction of information (...) that are necessary for fulfilling the task of state institutions. Therefore these provisions that follow a similar regulation concept as Reg. 40 and Reg. 106, are applicable to certain public sector personal data processing systems only which would leave open a gap for IT security measures in the non-public sector.

## OFFICIAL SECRETS

According to Section 4 of the Personal Data Protection Law The Law on Official Secrets can have an overriding effect. Section 4 subsection 2 of this Law states:

The following information may be recognised as an official secret:

14) information regarding the means and techniques for the protection of official secrets;

This means that certain security measures have to be handled according to the rules of the Law on Official Secrets.

## 1.2.2 WAY OF IMPLEMENTATION

The Latvian way of implementation of Art.16 and Art.17 of the European Dir. 95/46/EC deviates substantially from the Dir. abstract way of definition of the appropriate technical and organisational measures to protect personal data.

## DETAILED LEGISLATION

As explained above the regulation concept of the Dir. concerning the question which technical and organisational measures are appropriate is technologically and timely open.

---

<sup>23</sup> Note of Assitant to the RTA on a telephone call to Ms. Agnese Gusarova, Head of Legal Division of DSI.

<sup>24</sup> Regulation on Compliance with Technical Requirements for state information systems and

The measure have to be “state of the art”. “State of the art” depends on the actual threat in a certain processing situation at a certain time.

These conditions applied on an actual case show why the very detailed, comprehensive but never complete and not differentiated approach of regulation has deficits. Such measures are difficult to handle for the target group (Which measure has to be taken when?) and inflexible. They are difficult to update and as not all possible threats and risks can be taken into account never complete. Moreover the fast changing sector of IT security is usually overtaking the necessary law making process for an updated regulation of the Cabinet.

#### GENERAL CLAUSE AND BEST PRACTICE GUIDES

More adapted to certain situations, timely up-to-date and nevertheless detailed could be a different concept of regulation which includes a general clause similar to the one used in the Dir. and a reference to Best practice information of a trusted state organisation (e.g. DSI) in the Personal Data Protection Law.

### 1.2.3 PROBLEMS RELATING TO LEGISLATION

#### SCOPE OF IMPLEMENTATION

The current situation is quite likely not compliant with the Dir. as the link to the outdated Regulation opens an area where are no general IT security measures mandatory. Moreover it is doubtful if the listings of IT security measures really list all “state of the art” measures that might be necessary in certain situations.

#### UPDATING IT SECURITY REQUIREMENTS

Especially the time component of the Dir. “state of the Art” clause is not adequately taken care of in the current regulation concept. A quicker easier to update system of recommended or in certain situations mandatory set of best practices could serve thi target better.

#### EXPERTISE / TIME FRAME

Such best practices should be published in an easy to reach place (e.g. the internet) by an organisation with good IT security expertise which is able to judge IT risks, to classify them and to consult on security measures. All this has to be done within a short time from the occurrence of new IT risks.

#### INDEPENDENCE

Such organisation should be independent from business interests as well as state influences to maintain a risk and solution driven system of IT security.

### 3. TECHNICAL REQUIREMENTS REGARDING THE SECURITY OF PERSONAL DATA

#### 1.3 INVENTORY OF EXISTING TECHNICAL DOCUMENTS

##### 1.3.1 REGULATIONS:

Reg. No. 40

- Reg. No. 106 (outdated)

DSI Data Protection Handbook

British Data Protection Audit Manual

##### 1.3.2 DESCRIPTION

[INTENDED] COMPARISON WITH REAL CASES (CONTROLS)

As we haven't had the possibility to look into a real audit-report, (even that this was promised 2 times to us) we were not able to evaluate and compare the practise of technical controls.

ANALYSING THE EXISTING DATA PROTECTION AUDIT MANUAL

PREFACE

The DSI has compiled a "manual of audit of data processing systems", which describes a way to perform an audit of data processing systems with the focus on data protection/privacy issues.

Compared to Germany at present, in Latvia are no local data protection officers in private companies or governmental institutions, but Paragraph 6 of the Cabinet Regulations No. 40 „*Minimal Technical and Organizational Requirements for Personal Data Protection System*“ provides that every year the system supervisor carries out internal audit of personal data processing systems and prepares a report on the measures implemented in the field of information security.

Quote from the foreword of the mentioned manual (engl. translation):

„Section 26, paragraph two of the said Law provides that every year state and local government institutions submit to Data State Inspection an internal audit opinion regarding personal data processing systems (including risk analysis of the system), as well as a report on measures implemented in the field of information security, but Section 29, paragraph three, Clause 6 of the Law provides that Data State Inspection accredits the individuals wishing to carry out the system audit in personal data processing systems of state and local governments according to the regulations of the Cabinet of Ministers. On January 13, 2004, the Cabinet adopted Regulations No. 25 "*Procedure for Accreditation of Individual Wishing to Carry Out System Audit in Personal Data Processing Systems of State and Local Governments*".

The present methodology consists of an Audit Manual and several forms with the aim of helping the Data Supervisor to pay attention to the issues on the level of accordance. This Manual is intended to be of assistance for Data Supervisors wishing to carry out their system audits by themselves, or order them. The Manual contains the practical basic advice on the execution of audit that allows even for small organizations with limited auditing experience to carry out the audit of accordance.

The Manual is drafted on a theoretical level, and it should not be considered as a document with the help of which one can verify the accordance of a concrete personal data system with the requirements of the Law on Protection of Data of Natural Persons. Its aim is to help

establish the possible areas of discordance to which the Data Supervisor has to pay particular attention.”

### 1.3.3 EVALUATION

#### INTENDED AUDIENCE

This manual is intended for accredited internal and external auditors as well as for DSI staff members. It describes the preferred methodology of such audits and contains a lot of forms with already formulated questions.

#### STANDARDS CONFORMITY

The described methodology for the audit process is oriented at international standards (ISO 19011) for audits. The described strategy and procedures seems to be either adequate and also the result of experiences. It also contains an introduction with useful hints for auditors-to-be.

#### DEALING WITH IT-SECURITY

The manual covers some aspects of it-security and it-security measures especially in forms G.7. „Forms for audit of accordance: eight data protection principles – Seventh Principle“. The questions covered herein deal with

- Security Policy
- Unauthorized or Illegal Data Processing
- Loyalty of Personnel
- Destruction of Personal Data
- Contingency Planning – Unintentional Loss, Destruction or Damage of Personal Data

#### TECHNICAL IT-SECURITY MEASURES

Not covered in the manual are details on the subject of differentiated technical it-security means in general (e.g. firewalls, encryption or access control implementations). Some of such has been covered in the Cabinet of Ministers Regulations No. 106 „Regulations on information system safety“, which are referenced in Cabinet of Ministers Regulations No. 40 „Obligatory technical and organizational requirements for protection of personal data processing systems“, Point 2.

In this context, it is important to mention, that at present the Regulations No. 106 are not in effect anymore because an updated version / proposal was not accepted/signed by the Prime Minister.

The recently established E-Government Ministry is working on a proposal for state information systems which was sent in the last week of the activity.

I would suggest not to put too much technical details into the Regulations, but to define aims to reach and criterias/standards to measure/compare the adequateness.

#### IDENTIFYING CONFLICTING FIELDS OF DATA PROTECTION AND IT-SECURITY

Summing up: there is a lack of questions, hints and tips in the area of it-security in the manual but a few references to it-security standards (e.g. BS 7799). It would not make sense

to reinvent the wheel and start an own comprehensive list of it-security areas to be covered. Instead it would be good if the manual could refer to national or international standards for it-security in general – which at best are updated on a regular basis.

The focus in the manual should be put on the question „how to identify critical it-security areas“ and especially „critical (possibly) conflicting areas, where it-security means conflicts with privacy / data protection requirements“ and „what are the best practise solutions in these fields?“.

To reach this goal, we suggest to refer to the principles of „privacy enhancing technologies“ (PET) and to collect examples of good privacy friendly it-security practise in different areas.

## 1.4 FURTHER REQUIREMENTS

### privacy enhancing technologies

Especially in the field of it-security we often have to deal with different approaches to reach the goal „high level of security“ at the expense of privacy. Not to play one aim off against the other, the solution is to search for a „multilateral security“<sup>25</sup> solution.

The principles of privacy enhancing technologies are:

- Transparency
- Sparing use of data
- System data protection, in particular built-in data protection technology
- Personal data self-protection, i.e. empowerment and support of users in looking after and asserting their own data protection rights as far as possible
- Multilateral security, i.e. only minimal trust in others is necessary

Source: Hansen\_03

#### EXAMPLE: "CREDENTIALS"

A credential system is a system in which users can obtain credentials from organisations and demonstrate possession of these credentials. Such a system is anonymous when transactions carried out by the same user cannot be linked. An anonymous credential system is of significant practical relevance because it is the best means of providing privacy for users. Such a system is described in a paper by Jan Camenisch and Anna Lysyanskaya,

---

<sup>25</sup> Multilateral Security respects the interests of all participants. Even that one cannot always implement the complete protection objectives, with multilateral security the participants can express their requirements and negotiate them on demand.

titled "An Efficient System for Non-transferable Anonymous Credentials with Optional Anonymity Revocation".

#### THE IMPORTANCE OF APPROPRIATE RISK ANALYSES

According to Latvian Cabinet of Ministers Regulations No 40 "Obligatory technical and organizational requirements for protection of personal data processing systems" (issued according to Article 26 of Personal Data Protection Law), the data controller and the data processor must implement appropriate **organisational** and **technical measures** intended for the protection of personal data [...]. These measures must ensure an adequate level of security appropriate to the **nature of the data** to be protected and the **risks** represented by the processing [...]. The requirement for risk analysis is also found in Art. 16 and 17 Directive 95/46/EC.

The conclusion is that it is necessary to determine the "nature of the data to be protected" and the „risks“ involved in the first place to evaluate the appropriateness of the measures.

While it seems to be relatively easy to determine the "nature of the data to be protected" (e.g. see Annex "Protection Requirement Categories") it is a much more complex and work intensive process to carry out an appropriate risk analysis.

#### 1.4.2 CAPABILITIES BASED ATTACK TREE RISK ANALYSIS METHODOLOGY

Because of the complexity risk analyses can have, the approach of many security manuals (e.g. the German IT Baseline Protection Manual) is to provide just a (comprehensive?) catalogue of threats and (counter-)measures for low to medium security requirements, without in-depth risk analyses.

While this approach can be cost effective, it has some obvious shortcomings:

- \_ An overall unique requirement of only medium level security is assumed
- \_ No (reliable) conclusions can be drawn about the achieved security level (if any)
- \_ No (reliable) conclusions can be drawn about the remaining risks

With the focus on privacy, at the very least the processed personal data should be categorized to get an overview of the levels of protection required for the data processing from this perspective.

As a good compromise is the use of a categorization system<sup>26</sup> in combination with a plan describing the data flows. This can be used to define the areas of data processing where an individual risk analysis is indispensable (= every area with sensitive or confidential data).

---

<sup>26</sup>see document "Description of data security conformity evaluation systems used in Germany"

Traditional risk analysis is based on statistics (or experiences) which are often not meaningful in the (relatively new and) very rapidly developing IT security area. For example, it is not sufficient to estimate the risk (“likeliness”) of being the victim of a hacker by consulting statistics because new technologies invent new security risks. One is better advised to follow the precautionary principle, that

**“EVERYTHING THAT IS POSSIBLE (FOR A THREAT AGENT) WILL BE DONE”**

Therefore (in the IT-Security area) it makes more sense to determine the capabilities (money, tools, time) a threat agent has and the knowledge needed to break into a specific system.

The latter approach – if thoroughly followed - is much more appropriate and can provide you with an overview of the actual **achieved security level** (i.e. answering the question: “What effort is needed to break the weakest part of the security chain?”)

Approaches in this field of risk analysis are, for example, the Attack Tree-based analyses, described by security expert Bruce Schneier et al. and the more advanced capability-based Attack Tree methodology by Amenaza (see 3.2.3 Examples “Capabilities-based Attack Tree Analysis” for a more detailed description)

#### TOOLS FOR RISK ANALYSIS

Matching the German IT Baseline Protection Manual, a tool called gstool is available from: <http://www.bsi.bund.de/gstool/down.htm>

For risks analysis with the attack tree model, SecurITree from Amenaza is available from <http://www.amenaza.com/>

#### 1.4.3 EXAMPLES FOR IT-SECURITY RECOMMENDATIONS

The following recommendations act just as examples:

##### ABSTRACT

This paper is an approach towards a more in-depth security manual with focus on data protection / privacy. The areas discussed herein are meant as examples and are not comprehensive.

As there exists a lot of good security advisories, we don't try to reinvent the wheel, but instead we try to point out some often conflicting fields and best practise approaches to solve them.

This handbook is meant not only for it-security experts, but for administrators, data protection officers, auditors, it consultants, and last but not least decision-makers and executives.

#### GETTING THE OVERVIEW

As the first steps before analysing some areas in-depth, one should always make shure to get an overview of the organization, the processes and the data workflows. Therefor the

Audit-Manual from DSI is very useful and the audit approach described herein should be considered (if not already done).

The main steps in a nutshell are:

1. Getting the overview of the organization, the processes and the processed (personal) data.
2. Experts / Lawyers should check in this stage for conformity with the law of personal data processing.
3. Check for and take into account the privacy policy, security policy and risk analysis(\*)
4. Check the technical processes for adequate security and data protection measures.

While the audit process is described in detail in the audit manual, there are some additional points that need your care and attention.

These are in particular the type of risk analysis, security measures which could raise new data protection problems, the risks (of processing) personal data in backups, biometrics and some other risks in common it environments.

These areas will be focused in the following sections.

#### THREAT MODELING AND RISK ANALYSIS

Classical risk analysing methodologies based on statistics are common knowledge. But this methodology has some shortcomings in the fast changing it area where we often have no meaningful statistics or, in the case of new technologies, not even any historic data.

Another drawback of this classic method is the difficulty to describe the achieved security level in relation to an (potential) attacker.

Often the definition of the attacker is rigid and the expenses to do the same analysis many times for different types of attackers are fairly high.

Therefore an capabilities based Attack-Tree Methodology as proposed in section 3.2.1 is recommended. A Further introduction to the capabilities based Attack-Tree Model can be found in the Annex.

#### THE AUDIT-DATA TRAIL PROBLEM

Audit-data trails (also called log files) are of importance for system revision and post security analysis. While in many cases these log files contain personal data, there use must be exactly evaluated.

An important “privacy enhancing technology” for the analysis of audit-data trails is the proper use of pseudonymization and anonymization.

anonymization and pseudonymization

While the traditional security measures of encryption and password authorisation offer full data access to anyone with permission, data anonymization (pseudonymization) provides access to the relationships between the data, but not to the sensitive data itself.

Example:

A positive example is the OpenSource PseudoCoRe project for pseudonymization with conditional reidentification of logfiles. [Quote from the description:]

Description

Unix systems in many cases record personal data in log files. We present tools that help in practice to retrofit privacy protection into existing Unix audit systems. Our tools are based on an approach to pseudonymizing Unix log files while balancing user requirements for anonymity and the service provider's requirements for accountability. By pseudonymizing identifying data in log files the association between the data and the real persons is hidden. Only upon good cause shown, such as a proceeding attack scenario, the identifying data behind the pseudonyms can be revealed. We develop a trust model as well as an architecture that integrates seamlessly with existing Unix systems.

Related links:

- Pseudo/CoRe project page at sourceforge <http://sourceforge.net/projects/pseudocore>

## USER TRACKING TECHNIQUES

Tracking technologies are used to track a series of acts (or movements) which can be related to a person or a persons pseudonym. These tracks can be gathered even over a longer period of time and can therefore be used build a profile of that persons customs (e.g. customer habits), interests or movements.

In IT systems tracking technologies are often used in combination with web-cookies, web-bugs and logfile analyses (e.g. for reidentification of visitors on web sites).

The major problem in this scenario is the collection and aggregation of personal data on the server side, which are personal profiles. While these profiles are often collections of pseudonymous personal data, the pure ammount oft data makes it easy to reveal the identity of the pseudonym by correlation with other databases (not mentioning the possibility that a person reveals its identity oneselves). This may switch the before pseudonymous profile into an extensive personal file. Therefore such correlation is strictly unlawful. It is to examine if the extensive collection of personal data even under pseudonyms is in accordance with data protection law.

## REQUIREMENTS FOR BACKUPS AND BACKUP STORAGE

Backups of data are nessesary for many purposes e.g. fast recovery after data media failure or loss, archiving or perpetuation of evidence. Even if this are not all purposes for what one

may need a data backup, these are the most common ones. But for every purpose we have even more ways to achieve these goals.

For example to minimize the data which will be lost after a spontaneous disk failure it is important to have up-to-date backups of the data. This could be achieved by

1. using checksums for stored data against single bit or byte errors
2. local mirrors of the harddisks (RAID-1 or 5) against a single disk failure
3. remote mirrors of stored data against physical destruction of the system (e.g. by fire or water)
4. using storage media (e.g. tape drives) to hold copies of the data, where these tapes could then be kept at a safe place.

While the concept of tape backups is very common, it is often just seen as a data security measure and related insecurities through are easily overlooked.

Security and privacy is concerned, if the data is stored unencrypted on the backup media. As opposed to data access through the operating system, the data on a backup media can be accessed without any restrictions! That means an easy access for data spies or nosy staff members: they don't need to circumvent the access restrictions of the data processing system (which often requires some more technical capabilities) if they could get hold of a backup media.

So a good practise is to have regulations for backups that cover at minimum the following items:

- what kind of data is backed up by what system?
- is sensitive or personal data encrypted before backed up? [s. [6. Encryption technologies and algorithms](#)]
- who is responsible for the backup and who for the restore processes?
- where are the backup medias stored?
- How easy is it for a data thief to get hold of a backup e.g. by stealing or copying a backup media or even by executing the backup process to an own media? (This has to be dealt than within the [risk analysis](#) and the security manual)

#### CRYPTOGRAPHIC TECHNOLOGIES AND ALGORITHMS

If in doubt when to choose what encryption system/method/technology, you should start by categorizing what kind of data is to protect. The following list gives a short overview of different kinds of data and related cryptographic technologies:

category of data to protect	related cryptographic technology
content data transmitted over insecure networks	VPN (IPSec, pptp) or OpenSSH-tunnels
e-mail content transmitted over insecure networks	PGP/GPG or S/MIME (x.509)
web content transmitted over insecure networks	HTTPS (SSL/TLS)

category of data to protect	related cryptographic technology
Authentication data	Challenge Response (Kerberos)
to hide communications data record	Mix-systems, JAP (java anon proxy)
audit-trail data (logfiles)	anonymisation / pseudonymisation
local files or folders and complete harddisk partitions	symmetric encryption tools (PGPDisk, dm-crypto)

Other requirements might be the protection against alteration of data, against man-in-the-middle attacks, etc. To achieve these goals different methods like checksums, one-way hashes or digital signatures can be used. More in-depth information about

Generally speaking, the type of data-flows (transmissions) to be protected determines the method of protection and the asserted classification determines the cryptographic algorithms to be used. In this scenario it is important not to focus too much on the security of the crypto algorithm but to include also the security of the end users terminal among others.

Related links:

- Overview of VPN security <http://www.cites.uiuc.edu/vpn/security.html>
- OpenSSH <http://openssh.org/>
- Gnu Privacy Guard GPG <http://www.gnupg.org/>
- OpenPGP standard <http://www.openpgp.org/>
- S/MIME standard <http://www.imc.org/ietf-smime/>
- SSL / TLS <http://www.freesoft.org/CIE/Topics/121.htm>
- 

## BIOMETRIC DATA

The acquisition (collection), storage and use of biometric data is always to be evaluated under the aspects of data protection because biometric data consists very often of personal data. Depending on the type of biometric data the potential danger of misuse is fairly high.

Examples:

If biometric data should be collected, stored and used to authenticate a person the following aspects should be considered (e.g. to choose the best methodology):

1. The collection can be done without / only with the cooperation of the person in charge?
2. The biometric attribute is left unintentionally (finger print)?

3. The biometric attribute can be taken automated and unnoticeable (CCTV)?
4. The biometric attribute can be used to draw conclusions from? (illnesses, etc.)
5. ....

#### SECURE TERMINAL EQUIPMENT (WORKPLACE PC)

Nowadays the workplace computer is often the weakest part in the security chain. Therefore it needs specific attention particularly when it is used for accessing the internet as well.

The workplace computer (PC) is regularly used for the following tasks:

- 4) secure authentication of users
- 5) executing applications for internal tasks or for machine control
- 6) executing applications for internet based communications (web browsers, e-mail clients)
- 7) creation / production and work on documents (office suite programs)

Doing these tasks, the computer executes simultaneously internal applications (with access to sensitive internal data) and programs for internet communications (e.g. web browsers and e-mail clients). Because the workplace computer (PC) is normally set up for functionality not security, it is the ideal target for hackers.

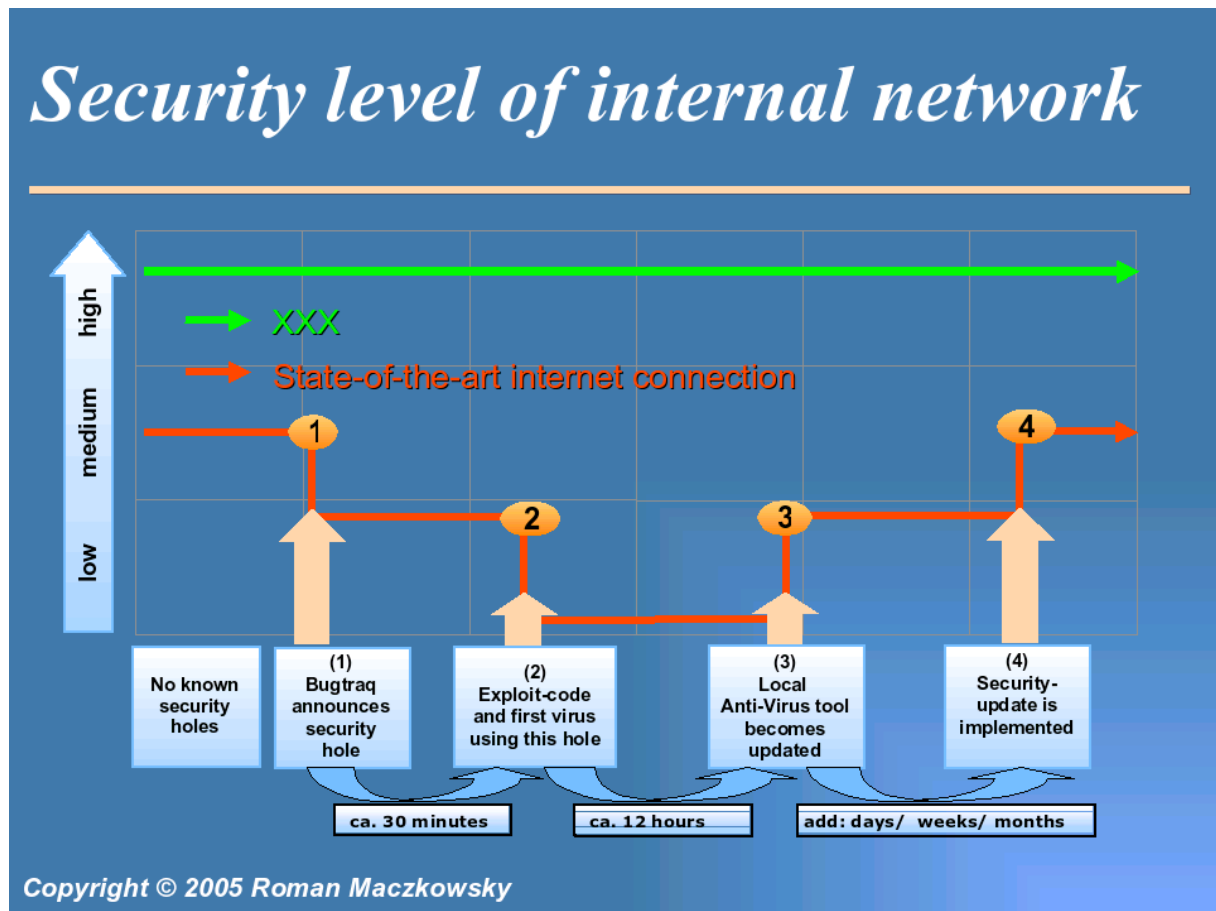
Through exploitation of a security hole in only one of the applications used for internet communication (browser, plug-in or e-mail client) or through "social engineering" an attacker can circumvent all installed security measures (firewall, anti-virus scanner) and access internal data!

The real cause for today's PCs being vulnerable to such attacks are on the one hand in the system architecture itself (shared Random Accessible Memory (RAM) for data and program code) and on the other hand in the access control models implemented in the operating system.

All common operating systems (MS Windows, Linux and Mac OS) use the discretionary access control (DAC) model. The DAC model only knows the (authenticated) user as user-id (uid) and his/her (file-)access rights. In the DAC-Model the uid (user) has the right to access specified files in a specified way (e.g. read, write, execute). All the files/programms the user executes then run also with the uid of this user – which in reverse means that every program started by the user is allowed to do everything the user is allowed to do – what includes: starting or stopping other programs, altering files, faking or capturing keystrokes and last but not least using the network capabilities.

Summarizing, this behavior is a matter of valid/permitted (though not always wanted) activity, which will neither be denied nor does it trigger an error or warn message.

Example: Attacking a system by an individual trojan horse programm (not detectable by virus scanners) and the proximate remote control of the attacked system through the firewall (permitted traffic)



### WIRELESS LAN SECURITY

Not to be tied to a physical cable but to take part in a local network seems not only comfortable but is sometimes a lot cheaper than to install cables and plugs.

On the other hand the “ease of access” is also the drawback of this technique. With a wlan, you open up your network to the public (or to the air). This makes some more security requirements necessary. Minimal requirements are:

- strong authentication for accesspoints and for mobile equipment
- strong encryption of all transferred data
- keep up-to-date with security discussions
- strong security configuration of wlan equipment to assure:
  - no fallback to weak or unencrypted modes
  - no insecure operating modes
  - no access to unidentified equipment
  - no access to any data without authorisation

- no access to reconfiguration over the wlan
- no possibility for man-in-the middle attacks

Of course this measures reduce the ease of use somehow but seems to be really necessary as controls in Hamburg, Germany impressively showed.

Related links:

- Wireless LAN Security FAQ: <http://www.iss.net/wireless>
- The Unofficial 802.11 Security Web Page: <http://www.drizzle.com/~aboba/IEEE/>
- Wardriving: <http://www.wardrive.net/>
- General introduction to wlan: [http://www.wlana.org/learning\\_center.html](http://www.wlana.org/learning_center.html)

#### WIRELESS DATA TRANSMISSIONS VIA BLUETOOTH AND IRDA

For other wireless data transmissions e.g. via Bluetooth or IrDA we can in general refer to chapter 8. (Wireless LAN security). The main differences are that Bluetooth and IrDA can only be used for (shorter) distances of 1 to 10 meters – which gives an other focus for an attacker – and that small equipment (like PDAs) often lack support for encryption and secure authentication.

IrDA defines a standard for an interoperable universal two way cordless infrared light transmission data port.

IrDA is utilized for high speed short range, line of sight, point-to-point cordless data transfer - suitable for HPCs, digital cameras, handheld data collection devices, etc...

The IrDA standards does not specify any security measures.”

In this field one has to weigh up the pros against the contras individually.

Related links:

- background information about Bluetooth system and security issues: <http://www.niksula.cs.hut.fi/~jiitv/bluesec.html>
- bluetooth device security database: <http://www.betaversion.net/btdsd/>
- bluetooth security white paper: [http://www.bluetooth.com/upload/24Security\\_Paper.PDF](http://www.bluetooth.com/upload/24Security_Paper.PDF)

## **4. RECOMMENDATIONS**

Generally the approach to give clear advice to public institutions and companies how IT security in the context of personal data protection should be implemented is very helpful. Nevertheless the current way of implementation of this approach is not supporting the aim of reaching an up-to-date level of IT security. Especially the close binding of updates to legislative or other official state measures should be abolished.

Therefore it would be helpful to find more flexible ways of distributing necessary IT security measures. We therefore recommend to change the current concept of implementing Art. 16. 17 Dir. by introducing a new general clause and a reference to best practices of reputable institutions in the Personal Data Protection Law. DSI could be one of these if the necessary manpower is available. Other Laws (i.e. the State Information Systems Law) could be included in this model.

The audit system can be considered an advanced mean of securing personal data protection and should be developed further according to the Latvian situation and new developments in IT security research. The attack tree model could be a general concept worth following.

## 5. ANNEXES

### 1.5 LEGAL PROVISIONS REGARDING THE SECURITY OF PERSONAL DATA

#### 1.5.1 DIRECTIVE 95/46/EC

##### ARTICLE 16 CONFIDENTIALITY OF PROCESSING

Any person acting under the authority of the controller or of the processor, including the processor himself, who has access to personal data must not process them except on instructions from the controller, unless he is required to do so by law.

##### ARTICLE 17 SECURITY OF PROCESSING

1. Member States shall provide that the controller must implement appropriate technical and organizational measures to protect personal data against accidental or unlawful destruction or accidental loss, alteration, unauthorized disclosure or access, in particular where the processing involves the transmission of data over a network, and against all other unlawful forms of processing.

Having regard to the state of the art and the cost of their implementation, such measures shall ensure a level of security appropriate to the risks represented by the processing and the nature of the data to be protected.

2. The Member States shall provide that the controller must, where processing is carried out on his behalf, choose a processor providing sufficient guarantees in respect of the technical security measures and organizational measures governing the processing to be carried out, and must ensure compliance with those measures.

3. The carrying out of processing by way of a processor must be governed by a contract or legal act binding the processor to the controller and stipulating in particular that:

- the processor shall act only on instructions from the controller,
- the obligations set out in paragraph 1, as defined by the law of the Member State in which the processor is established, shall also be incumbent on the processor.

4. For the purposes of keeping proof, the parts of the contract or the legal act relating to data protection and the requirements relating to the measures referred to in paragraph 1 shall be in writing or in another equivalent form.

##### RECITAL (46)

Whereas the protection of the rights and freedoms of data subjects with regard to the processing of personal data requires that appropriate technical and organizational measures be taken, both at the time of the design of the processing system and at the time of the processing itself, particularly in order to maintain security and thereby to prevent any unauthorized processing; whereas it is incumbent on the Member States to ensure that controllers comply with these measures; whereas these measures must ensure an appropriate level of security, taking into account the state of the art and the costs of their implementation in relation to the risks inherent in the processing and the nature of the data to be protected;

1.5.2 CONVENTION FOR THE PROTECTION OF INDIVIDUALS WITH REGARD TO AUTOMATIC PROCESSING OF PERSONAL DATA (ETS NO. 108)

ARTICLE 7 DATA SECURITY

Appropriate security measures shall be taken for the protection of personal data stored in automated data files against accidental or unauthorised destruction or accidental loss as well as against unauthorised access, alteration or dissemination.

### 1.5.3 LATVIAN PERSONAL DATA PROTECTION LAW

#### SECTION 26

- (1) The mandatory technical and organisational requirements for the protection of personal data processing systems shall be determined by the Cabinet.
- (2) Each year government and local government institutions shall submit to the State Data Inspection an opinion on internal audit of personal data processing systems (including system risk analysis, as well) and a report on measures taken in the sphere of information security. [24.10.2002]

#### SECTION 27

- (1) Natural persons involved in personal data processing shall make a commitment in writing to preserve and not, in an unlawful manner, disclose personal data. Such persons have a duty not to disclose the personal data even after termination of legal employment or other contractually specified relations.
- (2) A system controller is obliged to record the persons mentioned in Paragraph one of this Section.
- (3) When processing personal data, a processor of the personal data shall comply with the instructions of the system controller.

## 1.5.4 LATVIAN CABINET OF MINISTERS REGULATIONS No 40 (OF 30.01.2001)

## OBLIGATORY TECHNICAL AND ORGANIZATIONAL REQUIREMENTS FOR PROTECTION OF PERSONAL DATA PROCESSING SYSTEMS

Issued according to Article 26 of Personal Data Protection Law.

1. These regulations defines obligatory technical and organizational requirements for protection of personal data processing systems.
2. General provisions for protection of personal data processing systems is regulated by Regulations No 106 of Cabinet of Ministers "Security regulations for information systems".
3. Obligatory technical protection of personal data processing system is carried out with physical and logical protection means providing:
  - 3.1. protection against threats to personal data processing system caused by physical impact;
  - 3.2. protection which is realised with software, passwords, cryptography and other logical protection means.
4. Carrying out personal data processing system administrator shall provide:
  - 4.1. access to technical resources which are used for personal data processing and protection (including personal data) only by authorised persons;
  - 4.2. registration, transfer, arrangement, modification, transmission, copying and other processing of information carriers where personal data is saved is carried out only by exclusively authorised persons;
  - 4.3. personal data collection, saving, arrangement of saved personal data, storing, copying modification, correction, deleting, elimination, archiving, reserve copying, blocking is proceeded only by exclusively authorised persons as well as providing possibility to track down personal data which were processed without respective authorisation, as well as processing time and person which processed personal data.
  - 4.4. Transfer of personal data processing system using technical resources is carried out only by exclusively authorised person;
  - 4.5. When transferring personal data information should be registered on:
    - 4.5.1. personal data transfer time;
    - 4.5.2. person who has transferred personal data;
    - 4.5.3. person who has received personal data;
    - 4.5.4. personal data which are transferred.
  - 4.6. Inputting personal data, information should be registered on:
    - 4.6.1. personal data input time;
    - 4.6.2. person who has input pd in personal data processing system;
    - 4.6.3. person from whom personal data has received;
    - 4.6.4. personal data which are input in personal data processing system;
5. System administrator for each personal data processing system elaborates internal data processing system protection provisions, where are established:
  - 5.1. responsible person for personal data protection, their rights and obligations;
  - 5.2. personal data protection classification by its value and degree of confidentiality;
  - 5.3. technical resources by which personal data processing will be provided;
  - 5.4. managerial procedure of personal data processing, establishing personal data processing time, place and order;

- 5.5. activities which should be carried out for protection of technical resources in cases of emergency (fire, flood);
- 5.6. means with which protection of technical resources is provided against intentional damage and illegal acquisition;
- 5.7. order of storing and elimination of data carriers;
- 5.8. length of passwords and conditions on its structure (minimal length of password is 8 symbols);
- 5.9. regulations on password using, as well as period of time after what password should be changed;
- 5.10. action if password or cryptography key is got known by other persons;
- 6. System administrator each year carries out interior audit of personal data processing system and prepares overview of activities, which were performed in sphere of information protection.
- 7. System administrator informs persons, which processes the personal data on compulsory technical and managerial requirements for protection of personal data processing systems.

President of Cabinet of Ministers A.Berzins

Instead of Minister of Justice - Minister of Foreign Affairs I.Berzins

### 1.5.5 GERMAN FEDERAL DATA PROTECTION ACT

#### SECTION 5 CONFIDENTIALITY

Persons employed in data processing shall not collect, process or use personal data without authorization (confidentiality) . On taking up their duties such persons, in so far as they work for private bodies, shall be required to give an undertaking to maintain such confidentiality. This undertaking shall continue to be valid after termination of their activity.

#### SECTION 9 TECHNICAL AND ORGANIZATIONAL MEASURES

Public and private bodies collecting, processing or using personal data either on their own behalf or on behalf of others shall take the technical and organizational measures necessary to ensure the implementation of the provisions of this Act, in particular the requirements set out in the annex to this Act. Measures shall be required only if the effort involved is reasonable in relation to the desired level of protection.

#### SECTION 11 COLLECTION, PROCESSING OR USE OF PERSONAL DATA BY AN AGENT

(1) Where other bodies are commissioned to collect, process or use personal data, responsibility for compliance with the provisions of this Act and with other data protection provisions shall rest with the principal. The rights referred to in sections 6, 7 and 8 of this Act shall be asserted vis-à-vis the principal.

(2) The agent shall be carefully selected, with particular regard for the suitability of the technical and organizational measures taken by him. The commission shall be given in writing, specifying the data collection, processing and use of the data, the technical and organizational measures and any subcommissions. In the case of public bodies, the commission may be given by the supervisory authority. The principal must satisfy himself that the agent's technical and organizational measures are complied with.

(3) The agent may collect, process or use the data only as instructed by the principal. If he thinks that an instruction of the principal infringes this Act or other data protection provisions, he shall point this out to the principal without delay.

(4) For the agent the only applicable provisions other than those of sections 5, 9, 43 (1), (3) and (4) as well as sections 44 (1), Nos. 2, 5, 6 and 7 and (2) of this Act shall be the provisions on data protection control or supervision, namely for

1. a) public bodies,

b) private bodies where the public sector possesses the majority of shares or votes and where the principal is a public body, sections 18, 24 to 26 of this Act or the relevant data protection laws of the Länder,

2. other private bodies in so far as they are commissioned to collect, process or use personal data in the normal course of business as service enterprises, sections 4f, 4g and 38 of this Act.

(5) Paragraphs (1) to (4) shall apply mutatis mutandi where the testing or maintenance of automated procedures or data-processing systems is carried out by other bodies and the possibility of personal data being accessed cannot be ruled out.

#### ANNEX (TO THE FIRST SENTENCE OF SECTION 9 OF THIS ACT)

Where personal data are processed or used by automated means, the internal organization of the authority or the establishment shall be arranged in such a way as to meet the special requirements of data protection. In particular, measures appropriate to the type of personal data to be protected shall be taken

1. to prevent unauthorized persons from gaining entry to data-processing installations where personal data are processed or used (entry control),

2. to prevent the use of data-processing systems by unauthorized persons (access control),
3. to ensure that persons authorized to use a data-processing system can gain access only to the data they have authority to access and that personal data cannot be read, copied, modified or removed without authorization during processing, use or after being recorded (intervention control),
4. to ensure that during electronic disclosure or during transport or storage on data media, personal data cannot be read, copied, modified or removed without authorization and that it is possible to verify and establish to which bodies a disclosure of personal data by means of data disclosure equipment is planned (disclosure control),
5. to ensure that it is possible to verify and establish ex post facto whether and by whom personal data were entered into data-processing systems, modified or removed (input control),
6. to ensure that personal data being processed by a processing agent can be processed only in accordance with the principal's instructions (agent control),
7. to ensure that personal data are protected against accidental destruction or loss (preservation control),
8. to ensure that data collected for different purposes can be processed separately.

## **1.6 TECHNICAL DOCUMENTS REGARDING THE SECURITY OF PERSONAL DATA PROCESSING**

### **1.6.1 DSI DATA PROTECTION MANUAL**

Please find the English translation of the manual attached as a separate document.

### 1.6.2 PROTECTION REQUIREMENT CATEGORIES

The type and extent of data security measures depend, among other things, on the specific nature of the stored personal data. To better estimate the necessity of measures, it has proven helpful to classify personal data into categories according to the grade of their possible negative impact on interests of protection when misused. Data items must never be classified distinct from the file. The focus should rather be extended to the whole file or, where appropriate, also to directly connectible data. If personal data is collected under a specific criteria that itself is not in the file or database, this specific criteria must also be weighted in the process of classification. If files contain comprehensive data related to a person (Dossier) they must be classed into the next higher category as would be requisite by classifying the particularized data.

The distinguished categories are:

**Cat. A:** freely accessible data, where the requester does not need to assert his/her legitimate interest e.g. address books, member lists, user lists in libraries.

**Cat. B:** personal data, where one would not expect a specific negative impact in case of misuse, but where access is based on a legitimate interest, e.g. restricted-access public data, distributions lists.

**Cat. C:** personal data, where misuse could compromise the person concerned in their social status or in their economic circumstances (reputation), e.g. income, social security contributions, property tax, minor infringements, etc.

**Cat. D:** personal data, where misuse could significantly compromise the person concerned in their social status or in their economic circumstances (livelihood), e.g. institutionalization, criminal records, infringements, staff assessments, medical records, debts, impoundments, bankruptcy.

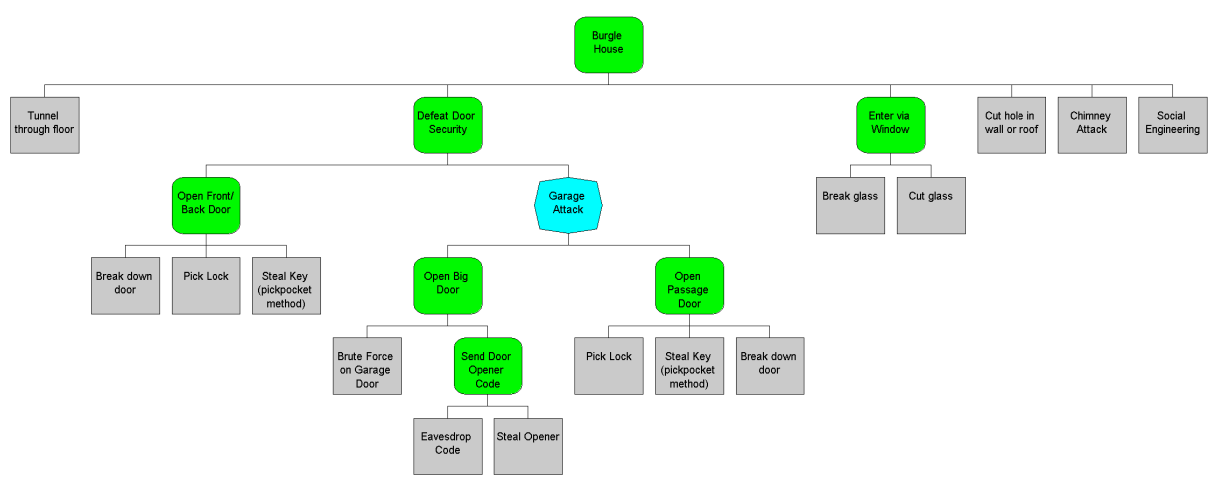
**Cat. E:** personal data, where misuse could compromise the health, life or freedom of the person concerned, e.g. data about persons who might become victims of a criminal offence.

If the sensitivity is unknown, the highest category must be assumed. It is also conceivable that a higher classification is recommended because sensitive business data are contained.

### 1.6.3 CAPABILITIES-BASED ATTACK TREE ANALYSIS

Attack trees graphically show how an asset can be attacked. The topmost (or root) node in an attack tree represents the attacker's goal. This overall goal is decomposed into nodes representing increasingly detailed tasks which, by themselves or in combination, will result in the attacker obtaining their objective. Associated with the detailed tasks are estimates, based on expert opinion, of the resources required by the attacker to perform the operation. Resources include money, technical ability, materials and how noticeable the attack is.

By estimating the capabilities of the adversary it is possible to eliminate those portions of the attack tree model that are unattainable. This greatly reduces the problem of defending the asset. Further analysis can show which of the remaining attacks are preferred by the adversary (i.e. bring them the greatest benefit and / or the lowest expenditure of resources) and which are most harmful to the victim. This allows a true determination of risk.



Copyright© 2001-2005 by Amenaza Technologies Limited. All rights reserved.

The following quote from Keith Brown is another good introduction to threat modelling.

#### “What Is Threat Modeling

Security is a lot about tradeoffs. Rarely can you apply a security countermeasure to a system and not trade off convenience, privacy, or something else that users of that system hold dear to their hearts. Bruce Schneier talks a lot about these tradeoffs in real-world systems such as airports ([Schneier 2000](#)). In computer systems, the same tradeoffs apply. Forcing users to run with least privilege (as opposed to administrators) is a huge hurdle that many organizations cannot seem to get past, for example, simply because it's painful for users. Most software breaks when run without administrative privileges (which is stupid and should be fixed, as I discuss in [WhatIsANonPrivilegedUser](#)).

It stands to reason that when designing secure systems, you should not simply throw random countermeasures at the design, hoping to achieve security nirvana, but you'd be surprised how often this happens. For example, there's something magical about the acronym RSA. Just because your product uses good cryptographic algorithms (like RSA) doesn't mean it's secure! You need to ask yourself some questions.

Who are my potential adversaries?

What is their motivation, and what are their goals?

How much inside information do they have?

How much funding do they have?

How averse are they to risk?

This is the start of a threat model. By sitting down with a small group of bright people who span a product's entire life-cycle (product managers, marketing, sales, developers, testers, writers, executives), you can brainstorm about the security of that product. Once you figure out the bad guys you're up against ([Schneier 2000](#) has some great guidance here), you can start to think about the specific threats to your system. Now you'll be asking questions like these:

Is my system secure from a malicious user who sends me malformed input?

Is my database secure from unauthorized access?

Will my system tolerate the destruction of a data center in a tactical nuclear strike?

I'm not being facetious here. Someone who asserts an unqualified "My system is secure" either is a fool or is trying to fool you! No one can say a system is "secure" without knowing what the threats are. Is your system secure against a hand grenade? Probably not. You can have security theater or you can have real security, and if you want the latter, you'll need to think about the specific threats that you want to mitigate. As you'll see, you'll never be able to eliminate all threats. Even if you could, you'd be eliminating all risk, and businesses rarely prosper without a certain margin of risk. Heck, if you disconnect a computer and bury it in 20 feet of freshly poured concrete, there's very little risk that anyone will steal its data, but accessing that data yourself will be a bit challenging. Real security has a lot to do with risk management, and one of the first steps to achieving a good balance between threat mitigation and ease of use is to know the threats!

But how can you possibly analyze all the threats in a nontrivial system? It's not easy, and you'll likely never find them all. Don't give up hope, though. Due diligence here will really pay off. Most threat models start with data flow diagrams that chart the system. Spending the time to build such a model helps you understand your system better, and this is a laudable goal on its own, wouldn't you say? Besides, it's impossible to secure a system that you don't understand. Once you see the data flows, you can start looking for vulnerabilities.

Microsoft has an acronym that they use internally to help them find vulnerabilities in their software, STRIDE ([Howard and LeBlanc 2000](#)):

Spoofing

Tampering

Repudiation

Information disclosure

Denial of service

Elevation of privilege

Spoofing is pretending to be someone or something you're not. A client might spoof another user in order to access his personal data. Server-spoofing attacks happen all the time: Have you ever gotten an e-mail that claims to come from eBay, and when you click the link, you end up at a site that looks a lot like eBay but is asking you for personal information that eBay would never request (like your Social Security number or PIN codes)? This attack is now so common that it's earned a specific name: phishing.

Tampering attacks can be directed against static data files or network packets. Most developers don't think about tampering attacks. When reading an XML configuration file, for example, do you carefully check for valid input? Would your program behave badly if that configuration file contained malformed data? Also, on the network most people seem to think that encryption protects them against tampering attacks. Unless you know that your

connection is integrity protected ([WhatIsCIA](#)), you're better off not making this assumption because many encryption techniques allow an attacker to flip bits in the ciphertext, which results in the corresponding bits in the plaintext being flipped, and this goes undetected without integrity protection.

Repudiation is where the attacker denies having performed some act. This is particularly important to consider if you plan on prosecuting an attacker. A common protection against repudiation is a secure log file, with timestamped events. One interesting consideration with these types of logs is the kind of data you store in them. If the log file were to be included in a court subpoena, would it be more damaging to your company to reveal it? Be careful what you put in there!

Information disclosure can occur with static data files as well as network packets. This is the unauthorized viewing of sensitive data. For example, someone running a promiscuous network sniffer such as NETMON.EXE can sniff all the Ethernet frames on a subnet. And don't try to convince yourself that a switch can prevent this!

Denial of service (DOS) is when the attacker can prevent valid users receiving reasonable service from your system. If the attacker can crash your server, that's DOS. If the attacker can flood your server with fake requests so that you can't service legitimate users, that's DOS.

Elevation of privilege allows an attacker to achieve a higher level of privilege than she should normally have. For example, a buffer overflow in an application running as SYSTEM might allow an attacker to run code of her choosing at a very high level of privilege. Running with least privilege is one way to help avert such attacks ([WhatIsThePrincipleOfLeastPrivilege](#)).

Another technique that is useful when rooting out vulnerabilities is something called an attack tree. It's a very simple concept: Pick a goal that an attacker might have—say, "Decrypt a message from machine A to machine B." Then brainstorm to figure out some avenues the attacker might pursue in order to achieve this goal. These avenues become nodes under the original goal and become goals themselves that can be evaluated the same way. I show a simple example in Figure 3.1.

```
GOAL: Decrypt a message from machine A to machine B.
1. Break the encryption algorithm and decrypt the message, or
2. Acquire an encryption key and decrypt the message, or
3. Read the message before it's encrypted on A, or
4. Read the message after it's decrypted on B.
```

Figure 3.1 Building an attack tree

You can continue the analysis by drilling down into each new goal (Figure 3.2).

```

GOAL: Decrypt a message from machine A to machine B.
1. Break the encryption and decrypt the message, or
2. Acquire an encryption key and decrypt the message, or
  2.1. Perform a brute force attack against the key, or
  2.2. If the key was derived from a password,
        perform a dictionary attack against the key, or
  2.3. Use social engineering to steal the key, or
        2.3.1 Phone someone in the organization, or
        2.3.2 Befriend an employee outside work
  2.4. Threaten someone to get the key
3. Read the message before it's encrypted on A, or
  3.1. Compromise the FOO service on A, and
  3.2. Elevate privilege by exploiting a bug in the BAR
service, and
  3.3. Read the process memory of the sending process on A.
4. Read the message after it's decrypted on B.
...

```

Figure 3.2 Further developing an attack tree

The beauty of attack trees is that they help you document your thought process. You can always revisit the tree to ensure that you didn't miss something. Entire branches of an attack tree can sometimes be reused in different contexts. [...]"  
From: <http://pluralsight.com/wiki/default.aspx/Keith.GuideBook/WhatsThreatModeling.html>

On the downside, conventional, checklist-based threat risk assessment (TRA) approaches are cumbersome, do not scale, produce recommendations that are hard to defend and are impossible to maintain in a timely fashion as the threat environment changes. Instead of that, "an Attack tree is a formal, methodical way of finding ways to attack the security of a system." [DDJ9912]

Quote from Amenaza (<http://www.amenaza.com/benefits.html>) "SecurITree attack tree analysis":

#### THREE KEY BENEFITS OF ATTACK TREE ANALYSIS

In the current security climate, the last thing professionals need is another time-consuming methodology for threat vulnerability assessment (TVA) or threat risk analysis (TRA).

Attack tree analysis cuts through the clutter by focusing first on how an attacker looks at your vulnerable systems. What does it cost them to ruin your day? With that information in hand, key organizational issues can be addressed:

##### 1 - Corporate Due Diligence

Security risks have many implications for a company. Not least of which is the liability incurred by a breach or disruption of service. Attack tree analysis provides one of the few clear and disciplined methods to prove to your customers and the courts of law that your company's behaviour was professional, timely and appropriate. SecurITree provides a simple method for tracking how your company identified potential risks, made cost-effective changes in policy or infrastructure to contain those risks ... and how the company responded through time to newly identified risks.

Keep in mind that customers and regulatory authorities have a legal stake in the security of your company!

## 2 - Validate Solutions Against Expectations

It's not just how much you spend on security solutions, it's whether or not that money does any good!

**Secur/Tree** identifies the key events that an attacker must accomplish in order to reach their goal. Their failure at those key events closes the door on them, no matter what else is done. Spend your money where it will do the most good ... and prove it to senior management!

If the boss or Board of Directors says that data security is the highest priority, use **Secur/Tree** to show exactly how the recommended solutions or changes will address that priority before all others. No more blanket solutions. Target your efforts to the things that actually count.

## 3 - Return on Investment - What are we getting?

With a clear methodology for corporate risk assessment, and a solid confirmation that proposed solutions will fix problems, the third key benefit of attack tree analysis is explicit justification. What kind of return on investment (ROI) are you getting?

**Secur/Tree** is a tool that explicitly declares how much time, effort and money an attacker must expend to successfully have an impact of a certain value on your company. The price to block that impact is also built into your attack tree analysis.

What's our return on investment? How much was spent to protect us against X dollars of damage?

Attackers are calculating their return on investment. Your company has to be just as focused ... spending money with a clear sense of what's effective and what's affordable.

Related links:

- Amenaza Technologies Limited <http://www.amenaza.com/benefits.html>
- Introduction: What Is Threat Modelling <http://pluralsight.com/wiki/default.aspx/Keith.GuideBook/WhatIsThreatModeling.html>
- Seminar material <http://antareja.rvs.uni-bielefeld.de/~made/Seminar/Attack-Tree/>

## References

DDJ9912      Doctor Dobb's Journal, December 1999, Schneier B: Attack Trees, pp 21-29

1.6.4 COMMENT ON THE “MANUAL OF AUDIT OF DATA PROCESSING SYSTEMS” BY STE DR. T. PROBST

Please find the English translation of the manual attached as a separate document.