There is no such thing as secure data

Refuting the myths of secure IT systems

Table of contents

1. What is this all about?

The amount of sensitive data being collected, saved and concentrated is increasing steadily. These collections are a severe threat to individuals, economy and society. The massive risks are usually underestimated, sometimes even unnoticed.

The sample cases from a professional hacker's life and some sample privacy scandals will give you a better picture of the existing threats.

2. A day in the life of a professional hacker

We hold a report from a professional hacker - an IT pentester and security expert. On behalf of big companies he has to break into their networks in order to discover security deficits.

In his report "Status quo analysis of practical IT security" he describes the real-life situation in data processing companies and gives practical examples. Insufficient qualification on the part of the responsible managers and engineers as well as staff shortages on the part of the investigating authorities are common reasons why attacks to IT systems often go unnoticed or are being recognized and stopped too late (six months and more).

Some simplified examples can be found in the following chapters.

Conclusions of the hacker

The professional hacker is in contact with us. We can arrange contact if necessary. In his report he comes to the following conclusions:

1. Status quo: It is not possible to give higly sensitive data appropriate protection.
   - Computer systems cannot be protected completely.
   - A successfull attack within short time is highly possible.
   - Even state-of-the-art security technology has severe flaws
2. The possible degree of it security is seldomly being achieved.
   - IT is too complex to be understood in every aspect.
   - For "best practice" reasons technical reality often differs from the theoretical concept.
   - IT systems usually are not separated consequently.
   - In order to make life easier, security often is weakened up.
3. There is a lack of communication between IT and non-technical staff
   - Non-technical staff usually assumes that everything is OK.
4. IT attacks require only basic knowledge that can easily be aquired on the internet.
   - Contrary to common belief, countermeasures are very complicated and difficult to implement.
5. Consolidated data storage is brittle.
   - Secure and authenticated access to data while trying to prevent abuse at the same time will not work in the long run.

Insecure, misuse-prone data are a widespread problem for society as well as for the economy.

Data misuse, loss and leaks pose serious threats to the existence of people as well as companies.

Contrary to conventional crime, consequences of data scandals oftentimes cannot be reversed.

Examples of personal/individual sensitive data:

- Income data
- Employer data
- Membership in trade unions, associations or groups
- Bank and payment data
- Consumer data
- Geographic and behavioral profiling
- Scoring
- Participation in witness protection programs
- Health data, medical files
- Tax and finance data
- Sexual preferences
- Political orientation
- Press contacts

Examples of sensitive data in economy, industry and research:

- Research projects, developments, patent applications
- Finance data
- Tax data
- Turnover/sales statistics
- Confidential communication
- Bidding/quotation data, purchase conditions
- Customer data
- Strategy papers, internal memos

2.1. All-finance group

Crime scene:

Large German all-finance group

Task:

Security assessment

Framework:

System administrators were not informed

Report:

The entry was secured by electronic ID cards. At the entrace visitors were being checked by security staff. We followed some employees while they were entering the building. People were holding the doors open for us. Afterwards, our team split up.

We looked for an available conference room and asked friendly in a nearby office whether the room was reserved and whether we could use it for the day. They gave us a key that we could use for locking up our notebooks over lunchtime. Starting off from this room, we started the on site pentest. Because we did not want to raise attention, we were proceeding slowly and carefully. After roughly 3 hours we got access to a delinquency procedure database by redirecting data packages. Furthermore we had access to a fileserver and several passwords. As the evening came, we had administrator privileges on some end user systems by exploiting weaknesses that allowed us to switch users.

The next day, we cracked all HQ employee's passwords except for ca. 100 within 45 minutes. We discovered several leaks. Furthermore we were able to execute tasks by using stolen identities.

In a real attack, most likely the employees would have been the main target for investigations. At the third day we decided to act more openly. Our attack was being discovered at the end of the third day when we deactivated the virus scanner on a central system. Although IT security staff did a careful research, they found nearly nothing. They came to the conclusion that a service account password had been stolen.

Our second team went through the building pretending to make an inventory of all hardware for the IT department. Instead they installed keyloggers and accespoints and took away files lying around on desks. They collected faulty printouts which had been trashed and copied documents from the department printer's buffer. During the whole day my colleagues were leaving and entering the site several times. The team even got access to the data center by pretending to check fire security. At the second day the team was stopped by an employee who correctly informed securiy staff. The site security member arrived a few minutes later and asked the caught-in-the-acts to follow him to his office. On the way the team told him about their task to make an invetory of all computers. This was reason enough for the site security member to hand out a general access card without asking his manager or any contact person.

Conclusion:

- Site access possible despite latest security hardware
- Once inside, unlimited access to all parts of the building
- Insufficient employee awareness
- Access to critical data within 3 hours
- Administrator privileges on the first day
- Simple and poorly protected passwords
- Severe weaknesses in application security
- IT security did only shallow investigations without proper results

2.2. Technology company

Crime scene:

International specialist for industrial process technology

Task:

Security assessment, on site pentest

Framework:

System administration has not been informed

Report:

The building was entered through the main entrace without any control. Inside the building, the different departments were protected by RFID systems but it was possible to get anywhere by simply slipping through the door tailgating an employee. Although they usually asked who we are and what we do they were easily satisfied with simple explanations like "fire alarm control" or "computer inventory". We installed several access points and keyloggers. In several conversations with employees, my colleague got hold of their passwords while I was sitting under the desk, preparing their computers.

In the evening after the main entrance already had been closed and the cleaners were doing their job, we knocked at the door until someone opened. We asked him to let us in and told him as an excuse we urgently had to install some hardware and had forgotten our ID card. After the cleaning staff member called his manager, he let us in. One chief executive was still in the building. We told hin the excuse that we had to perform some tests and installed some (dummy) software on his machine.

During on site pentest we got access to critical information and administrative passwords within very short time. This was due to bugs in the operating system of the network component of a rather famous manufacturer which gave us access to data of other networks and extensions without further attacking the system, even though the seperation was configured correctly (by VLANs).

Furthermore, it was possible by simple means to connect to one of the allegedly physically seperated networks (VLAN). We had no permission to examine the R&D network. Nevertheless it was feasible to wiretap the phonecalls of all telephone extensions systematically (tested on two sample calls).

On the second day an IT staff member showed up and replaced the faulty switch due to "warning notices". The attack, properly detected by the hardware, had been declared a "defect" by the IT staff.

Conclusion:

- Site access possible despite latest security hardware
- Once inside the building unlimited access to every part despite latest security hardware
- Unsufficient employee awareness
- Access to critical data after 3 hours
- Admin access on the first day
- Simple and poorly protected passwords
- Massive vulnerabilites on application level

2.3. IT Service Provider

Crime scene:

IT service provider in a big German production and trade company

Task:

Security assessment, off site pentest, phishing attack, on site pentest, social engineering

Framework:

Administrators had been informed

Report:

Every part of the building could easily be entered. In the basement, there was an unlocked archive with all drafts, patents, blueprints, bills and all other printed information of the last 15 years. Installation of keyloggers and access points could be done with ease. Even in R&D department with highest safety requirements we could install an access point and a keylogger. Within a few minuts we had system and SAP access via our access point.

We left the hardware installed for 2 weeks. Although the employees became aware of the access points, they thought they were radios or parts of the long announced phone system.

During off site assessment we found several opportunities for SQL injections that allowed us to get into the internal customer's network. Furthermore we found a web site being hostet within the customer's IP range that the administrators did not know about.

Moreover we performed a phishing attack. The employees were asked to log in on a portal in order to coordinate a date for the end-of-year event. The first replies came in within the first minute. After 3.5 hours the phishing attack has been discovered.

During on site pentest we got access to production, development and finance systems. Most interesting were some maintenance accounts that allowed access to networks of the company's customers.

Conclusion:

- Entering the building and and high-security wing was possible with ease
- An unsecured paper archive is an additional risk
- Installation of spy hardware was possible
- Installed spy hardware has not been detected for 2 weeks
- Detected spy hardware has not been examined
- Access to critical information within very short time
- Access from outside was also possible
- Access to customer networks possible
- Phishing succeeded within a few minutes

2.4. Medical Service Provider

Crime scene:

Medium-sized medical software and service provider who is processing highly sensitive patient data. To fulfill his task, the software provider has access to his customer's production systems.

Task:

Security assessment, off site pentest, phishing attack, on site pentest, social engineering

Framework:

System administrators have been informed. Keyloggers and access points were not wanted.

Report:

The phishing attack was performed in two waves. Because it was technically impossible to send emails with internal sender's addresses to internal recipients, we used one IT staff member's webmail address. In the first wave we addressed 32 higher management and IT staff members, telling them about a new portal. Within 30 seconds, the CEO did enter his password. Before a warning had been sent out, 29 employees had answered.

In the second wave one week later, we sent emails to the same target group, containing a link to an alleged security update and this text: "Due to last week's phishing attack we ask you to install the following patch." Actually the link let them install a trojan horse that was simply increasing a counter. We counted 11 installations. A real trojan horse would have opened permanent access to customer networks.

During off site assessment we only found a few services available on the internet. Most services were hosted at an external service provider. There were some low-level security holes that were fixed immediately.

The access to the building was controlled by site security that was handing out visitor badges. We passed the guard saying a friedly "hello".

The elevator could only be unlocked with RFID tokens, so we decided to take the staircase. Up to the fourth floor every wing was also protected by RFID tokens. In the fourth floor there was a big metal door with a bell. After we rang it, the door opened and we came into a small turnstile with a CCTV protected second door at the end. After that door was the reception desk. We passed the reception, pretending an intensive discussion. As we found out later, the women at the reception was slightly puzzled, but because we were passing here so thrustingly she didn't know what to do. Se did not consider a malicious attack. We looked for a cleaning staff member and let her activate an elevator for the fifth floor.

During on site pentest we gained administrator privileges within 3.5 hours, thus allowing us access to all systems. Within 30 minutes we cracked all passwords except 2.

Conclusion:

- Despite turnstile hand high-level security measures foreigners could enter.
- The reception desk staff was not prepared to be ignored.
- A major part of the employees (29 to 32) including skilled staff fell into the phishing trap.
- Despite being warned 11 employees fell into the same trap again
- Access within half a day
- Passwords were too weak

2.5. Real Estate Investor

Crime scene:

A successful investor on the German real estate market

Task:

Security assessment, off site pentest, phishing attack, on site pentest, social engineering

Framework:

The system administators have not been informed

Report:

We found out later that unluckily the off site assessment took place during a maintenance window. Because all systems had been switched off, we found no attackable services on the internet.

During our phishing attack 2 employees gave away their password. Due to the maintenance window this also happened on the next day.

The first social engineering for checking the physical security was executed by two of my colleagues. In all departments they succeeded in installing keyloggers and access points.

During on site pentest we succeeded in accessing the complete rent database (prices, lodger's addresses, back rents, etc.), within two hours. Usually access was done through a frontent that tested entries for plausability. The direct database access allowd us to circumvene this test (i.e. to redeem back rents or to decrease rents without log entries). During the day we also got access to all core applications and file stores.

Our task was even more interesting because the company IT had already gone through a internal security audit. They claimed to have fixed several issues, but we were not able to reproduce this.

At the end of the on site test we performed a second social engineering to test the physical security in order to collect our previously installed equipment. With a little help from employees and cleaning staff it was possible despite of modern electronic access control to get into all departments between 8 and 10 pm and to collect hardware.

Conclusion:

- Access was possible within a short period of time
- Phishing attacks succeeded
- Free access to all parts of the building also after regular working time

2.6. Production within a major corporation

Crime scene:

Production company of a big German corporation

Task:

Security assessment, off site pentest, social engineering

Framework:

Administrators were informed; it was requested not to use key loggers or access points.

Report:

First, an off site pentest via internet was conducted. Access to core system from the internet was possible. The systems weren't hardened. After 40 Minutes we had gained administrator rights on the systems and could access the internal network.

A test on location (on site pentest) showed that because of incomplete network separation, complete access to other firms within the corporate group was possible.

While assessing physical security and vulnerability to social engineering, we had access to all areas and picked up documents as well as data media.

During the phishing attack 12 users were contacted, of which the first sent in his password within two minutes. 8 out of 12 users answered in all.

Conclusion:

- Access to the building was possible
- Accessing critical systems via internet was achieved in next to no time
- Access to internal systems and other areas within the corporation due to insufficient network separation
- Phishing successful in no time

2.7. Media group

Crime scene:

Major German media group

Task:

Testing an internet terminal in the entrance area

Framework:

The terminal was supposedly separated physically from the corporate network

Report:

Without preinstalled software, we gained access to an internal terminal server within six minutes. Switching between different login identities was possible. After some 45 minutes, we had gained administrator's rights as well as access to the publishing system (?) and a server containing financial data.

After about 90 minutes the mission was declared accomplished as we had reached our goals.

Conclusion:

- Access to the corporate network was possible within a few minutes.
- The alleged network separation was inefficient as a few services seemed to be routed.
- No special tools were needed for the attack.

2.8. Arms firm

Crime scene:

Subsidiary company of an American arms group

Task:

Security assessment, targeted validation of the configuration on location

Framework:

Administrators were informed

Report:

It was possible to log confidential data and passwords via network here as well. We gained access to all primary data bases and all server systems

We also noted that administrators circumvented security procedures, such as scheduled change of passwords, by technical tricks.

The company had a strict application procedure for user accounts. This was leveraged by massive multi-usage of existent accounts.

Conclusion:

- Access to all data was possible.
- Effective security measures were evaded even by administrators
- It was possible to install software unnoticed

2.9. Security specialist

Crime scene:

Security firm

Task:

None - security gap was noticed by chance while using the internet portal

Framework:

Unspecified

Report:

The security gap we accidentally found allowed access to data of a huge number of clients, including some major corporations, banks and government institutions of different countries.

The gap could be exploited simply by using a web browser. It's a standard recommendation not to rely on one individual security measure alone but rather to combine different measures. Practice shows that this isn't always the case. Thus access to lots of client data can be deemed probable.

The firm reacted within a few hours. Nevertheless a malicious attacker could have induced immeasurable harm.

Conclusion:

- Not even security specialists are immune against security flaws.
- A small number of vulnerabilities at central providers allow for the manipulation of large numbers of systems.
- Individual awareness for security issues doesn't immunize against attacks via software firms, service providers or other interfaces.
- Data vulnerability

3. Data misuse is possible, and it's taking place

Data is being misused on a daily basis. Contrary to conventional cases, in the IT environment data loss happens on a large scale. The following examples of serious events will provide an insight to what is possible and what is happening.

Data misuse as described here hardly ever comes to light. Past events often only came to public attention because of insiders' whistleblowing years after the actual event.

3.1. Deutsche Telekom / German Telekom

Crime scene:

Germany, Deutsche Telekom, one of the leading German telecommunications service providers

Time of the crime:

2006 to 2008

Victims:

About 17 million customers, critical journalists

Report:

In 2006, 17 million sets of customer data were stolen from Deutsche Telekom, among them secret phone numbers of ministers, politicians, former german heads of state/presidents, economic leaders, billionaires and church officials.

Deutsche Telekom hired private investigators to evaluate media coverage: Especially critical or investigative journalists were put on a list, the top five on this "charts list" being spied on for months.

On top of that, Telekom illegally snooped on connection records of about 60 individuals – using its very own data pool as well as that of a domestic competitor and of a foreign company.

In May 2008 the entire scandal surfaced. Five managers and employees were being relieved from their duties and sent "on vacation".

Conclusion:

- Large-scale, profound misuse of sensitive connection records by the leading German provider
- Revelation through a whistleblowing individual only

Source:
http://www.telekom.com/dtag/cms/contentblob/dt/de/812996/blobBinary/dt_open_book_abschlussReport.pdf
http://www.zeit.de/online/2008/41/telekom-datenklau

3.2. Deutsche Bahn AG

Crime scene:

Germany, Deutsche Bahn AG, a (so far) publicly owned transportation company, predominantly operating most of the german railway transportation.

Time of the crime:

2002 to 2009

Victims:

About 173,000 employees, unionists, journalists, one member of the federal government (Bundestag)

Report:

In the beginning of 2009, it became known (through the work of investigative journalists) that Deutsche Bahn had systematically monitored around 70,000 to 80,000 employees in 2002 and 2003. On a daily basis, 150,000 E-Mails were inspected. It was not until October 2008 that this activity was stopped.

For 173,000 out of their 240,000 employees, Deutsche Bahn had given data to private investigator firm "Network Deutschland". Based on address data and banking account details the investigators were supposed to check whether employees were carrying out business on the account of Deutsche Bahn. To accomplish this, their data were compared to data of 80,000 contractors.

Furthermore, Deutsche Bahn repeatedly compared it's employees' basic data (among them mailing address, telephone numbers and banking account data) to other databases.

The goal no longer being revealing corruption by questionable methods, but apparently mail monitoring was used to prohibit an undesired flow of information such as information concerning strikes of unionists from Gewerkschaft Deutscher Lokführer (GDL, union of german locomotive drivers).

GDL officials noticed their mails did not reach their destined addressees. Employees' electronic mail sent to critical journalists was retrieved as well as communication with scientists and traffic specialists, among them a member of the german federal parliament (Bundestag) who had publicly announced his criticism of Deutsche Bahn.

In the course of investigations, cases of bank accounts, private contacts and further personal information being collected and evaluated came to light. For example, video recordings of gas stations used by employees were retrieved.

Further investigating several cases, it is being reported that data of employees were manipulated, these manipulations subsequently being used to lay off critics of former chairman Mehdorn. Revising some payments, trade union "Transnet" had also requested two comparisons between their members' and employees' data.

In at least nine cases, a Berlin-based "research agency" had been hired to investigate employees, their spouses, contractors and other parties.

In May 2009 it became public that Deutsche Bahn's compliance manager had data shredded in January 2009 to hush up the affair.

Conclusion:

- Serious data misuse
- Slowly progressing, reluctant revelation
- "Successful" cover-up through the destruction of incriminating data

Source:
http://www.heise.de/newsticker/meldung/Bahn-soll-jahrelang-150-000-Mails-pro-Tag-gefiltert-haben-209988.html
http://www.heise.de/newsticker/meldung/Bahn-soll-Mitarbeiter-Mails-systematisch-durchforstet-haben-209878.html
http://www.heise.de/newsticker/meldung/Datenaffaere-Gewerkschaften-verlangen-von-Bahn-Chef-Entschuldigung-204214.html

3.3. Einwohnermeldeamt (residents' registration office)

Crime scene:

Germany, several government agencies

Time of the crime:

2008

Victims:

German residents in 200 cities and communities

Report:

In Germany, every resident is obliged to register with the registration office (Einwohnermeldeamt) of the district where they have their main place of residence. Quite a few personal data are collected and stored in a decentralised manner.

Following some human as well as technological malfunction in the registration office of Potsdam (near Berlin), these partly intimate personal informations were publicly available over the internet in spring 2008, with no protection whatsoever.

What had happened?

After the installation of software for the population register, employees failed to change the provided default password. For demonstration purposes though, the software manufacturer had been providing this password through its web site. Thus it was possible to access the actually strictly confidential data base. According to statements on behalf of the software manufacturer, overall 15 local authorities were affected by the data glitch.

Even prominent Potsdam inhabitants such as TV anchorman Günther Jauch, actress Nadja Uhl or fashion designer Wolfgang Joop's model-discovery Franziska Knuppe could have been spied out based on the screwup.

Conclusion:

- Simple misfortune leads to a far-reaching exposure of sensible, non-public data
- Disclosure through investigative journalism

Source:
http://www.heise.de/newsticker/meldung/Gut-dass-es-passiert-ist-Datenpanne-zwingt-zum-Umdenken-216194.html

3.4. Polish press scandal

Crime scene:

Poland, police and two major intelligence agencies

Time of the crime:

2005 to 2007

Victims:

At least 10 wide-known, influential journalists and their contact persons

Report:

Key Polish daily newspaper – Gazeta Wyborcza – discovered in October 2010 that at least 10 influential journalists were subjected to on-going surveillance in the years 2005-2007, i.e. at the time when conservative, right wing party ruled in Poland (PiS). The police and two major intelligence agencies, namely Central Anticorruption Bureau and Internal Security Agency, requested the data retained by telecom operators (traffic and subscribers data) in order to reveal their journalistic sources. Data was accessed by the police and secret services without any judicial control and beyond any legitimate procedure, i.e. not in relation to any pending criminal case. In this context it is clear that the use of traffic and subscribers data was not legitimate and constituted an outrageous example of data mining as well as the breach of journalistic confidentiality.

As a result of these actions, police and secret services were able to trace back journalistic sources. Purportedly some people from the administration and police lost their jobs when it was discovered that they contacted the journalists while working on politically controversial subjects. This abuse led to prosecutor's investigation aimed at finding out whether illegitimate surveillance of journalists did occur. Both police and secret service keep denying this. The investigation was allegedly closed due to lack of evidence. One of the journalists appealed against this decision and won the case in court. The court ordered that the case be re-opened and investigated in depth.

Conclusion:

- Data retention was used in order to reveal journalistic sources
- Without any judicial control and beyond any legitimate procedure
- Police and secret services were able to trace back journalistic sources
- This abuse of the right to privacy and journalistic confidentiality led to prosecutor's investigation
- The investigation was first cancelled for lack of evidence, to be re-opened only because a journalist stood his ground.

Source:
http://tvp.info/informacje/polska/inwigilacja-dziennikarzy-zamiatana-pod-dywan/3424956
http://wyborcza.pl/1,75478,8842563,Inwigilacja_dziennikarzy_badana_od_nowa.html

3.5. Operation Pecunia

Crime scene:

USA, Great Britain, Germany

Time of the crime:

1999 to 2007

Victims:

Several tens of thousands of false suspects – wrong accusations lead to 39 suicides!

Report:

A young navy general and 38 further persons in England committed suicide after having been accused and in part convicted of the acquisition of child pornography based on data trails. The young navy general was relieved of duty even though accusations based on the preceding investigations had not been confirmed.

The large-scale police operation "Operation Pecunia", also known as "Operation Ore" had its start in 1999 in the USA and concerned several tens of thousands of alleged consumers of child pornography.

From April to May 2007 it was exposed that a big part of the 7,000 suspected britains had been victims of credit card fraud; among them several of those having committed suicide. Their credit card data had been retrieved through "phishing" and used to gain access and pay for child pornography web sites. Whether an actual retrieval of pictures or videos had been taking place or if it was a case of money laundering, has not been clarified.

Suspects had been charged and in part convicted based on inadequate evidence.

Conclusion:

- Mass false accusations with a deadly outcome

Source:
http://oraclesyndicate.twoday.net/stories/4122817/
http://en.wikipedia.org/wiki/Operation_ore

3.6. Misuse of data retention in the Netherlands

Crime scene:

The Netherlands, law enforcement agencies and public prosecutor

Time of the crime:

2009

Victims:

A Dutch research journalist, a Dutch security expert, six friends of the research journalist

Report:

A Dutch research journalist exposed security weaknesses in the e-mail account of the State Secretary of Defense, Mr. Jack de Vries. The journalist did not publish any of the sensitive information he encountered, but informed the authorities about the possible dangers for the Dutch national security and later published an article about it in 'Nieuwe Revu', a Dutch magazine. Rather than relief that this had been discovered by a well-meaning journalist, the authorities reacted with prosecution.

In trial, the journalist found his entire telecommunications history in his file, including his anonymous sources in unrelated articles. He even discovered the entire telecommunications history of his friends bearing the same first name as the security expert that had helped him in his dossier – even though the name and the employer of the security expert could be found in the article, thus providing alternative and less intrusive means to reconstruct his identity. So the first names of all the contacts of the journalist had been reconstructed by the authorities through the CIOT-database, a Dutch national database that contains the subscriber data of each and every telecommunications user in The Netherlands.

The journalist was, of course, not convicted but tells us he feels intimidated to write such articles in the future.

Conclusion:

- Data retention revealed anonymous sources of the journalist in unrelated articles.
- Access to telecommunications data is requested, not because it's necessary but just because it's easy.
- Telecommunications data are requested of unrelated persons who have nothing to do with the investigation, only because they share the first name of a suspect.
- Through data retention, every single person can become a suspect in an investigation - only because they share a first name with a suspect.

Source:
http://www.edri.org/files/Data_Retention_Conference_031210final.pdf

4. Complex IT systems are ultimately beyond control

4.1. Tax Identification Number System

Crime scene:

Germany, everywhere

Time of the crime:

2007

Victims:

An unknown number of German citizens

Report:

The "Steuer ID" (Tax Identification Number) is a unique identification number for fiscal purposes, introduced on 1. July 2007.

This identification number is highly controversial among constitutional lawyers in fear of it mutating into a unique personal ID which has been banned by the German federal constitutional court (Bundesverfassungsgericht).

During the allocation of the tax numbers it turned out that not only outdated data had been recorded (alone in Stuttgart over 15,000 letters with the statement of tax-ID could not be delivered).

It turned out that the IT system was full of errors which led to a nationwide data mess.

Citizens were assigned false birth names, turned into foreigners, their places of birth displaced. Extraordinarily high was the error rate in Stade (near Hamburg). "A felt 100% of notifications sent out had errors attached to them", the lower-saxonian city's vice mayor Dirk Kraska says in a comment to news website 'heise online'.

Kraska himself was - following his assignment - Lebanon bred and his birth name was 'Solonin'. As reported by German newspaper 'Bild-Zeitung', the pensioner William Young was renamed to William Ficken and his birthplace was called 'Hamburg, Kazakhstan' from now on. Astrid Brauer allegedly stems from Iran, her husband from Russia and their son from Spain.

"We are clueless as to where the problem might be", Kraska adds. The city's residents registration office sent a CD to the responsible tax authority (Bundeszentralamt für Steuern) so manipulation while transferring data through the internet could be ruled out.

Conclusion:

- A huge number of state databases in a sensitive context are in very poor condition.
- That scandal has only been revealed because people got noticed of their faulty data.

Source:n
http://www.heise.de/newsticker/meldung/Kommunen-melden-grobe-Fehler-bei-Ausgabe-der-neuen-Steuernummer-195197.html
http://www.heise.de/newsticker/meldung/Bundesweit-Pannen-beim-Versand-der-neuen-Steuernummer-201607.html

4.2. The new electronic identity card

Crime scene:

Germany, everywhere

Time of the crime:

2010

Victims:

Numerous German citizens

Report:

Starting 1. November 2010 Germany issued a new piece of identification: the electronic identity card (elektronischer Personalausweis, E-Perso). This identity card is equipped with an RFID radio chip that contains identification data, biometric features of the owner's face as well as mandatory fingerprints and an additionally mandatory "qualified electronic signature".

To speed up acceptance of the new technology a group of citizens got free reading devices, worth 16 millions of Euros. It turned out that these devices, when connected to personal computers, led to serious security problems - including identity theft.

A while later, after the identity card had been introduced, an IT expert found out (on his own initiative) that the software provided by the federal authority featured a severe vulnerability that could have been exploited by trojan horses.

Shortly after, data glitches occured because of false names having been recorded to the identity cards.

Finally, in mid December 2010, it turns out some of the new identity cards had accidentally been equipped with empty radio chips. Additionally, the card's lock code that normally should have prevented unauthorized transmission and restrict the access to certain data was not functional.

Conclusion:

- Numerous data breakdowns in an IT project, organized by the state itself.
- Revelation of these circumstances by affected citizens, dedicated IT experts and one NGO

Source:
http://www.heise.de/newsticker/meldung/Fehlerhafte-Personalausweise-in-Hessen-1141762.html
http://www.heise.de/newsticker/meldung/Stotterstart-des-neuen-Personalausweises-1145554.html
http://www.heise.de/ct/artikel/ePerso-Alltag-Vom-Foerdern-und-Fordern-Update-1147116.html
http://www.mdr.de/nachrichten/7979773.html

4.3. The electronic health care card

Crime scene:

Germany, everywhere

Time of the crime:

Starting 2004

Victims:

Potentially all German citizens

Report:

As a major national project, the electronic health care card (elektronische Gesundheitskarte, eGK) is supposed to unify the acquisition and maintenance of health-related data while providing attending professionals with an easy and efficient interface to access health-related data. The billing of treatment expenses, data management and prescriptions are supposed to be simplified and speeded up.

The German Bundesregierung specifically founded an enterprise named 'Gematik' which was in charge to organize and implement this very ambitious IT project.

After having already set the implementation of the card by law in 2004 for 2006, until now - 2011 - nothing happened.

Aside from allocating costs of some hundreds of millions of Euros to date, no working or even satisfying infrastructure has been set.

Several field tests were not satisfactory or had to be cancelled. Among physicians, pharmacists and health insurance companies the acceptance is poor; the technical implementation has proven to be impractical or impossible.

As a result, the requirements for the card have been lowered on and on. Until now, there is no political courage to abandon the project though. Instead, the card's implementation is to be forced by law.

And we haven't even mentioned all the privacy related aspects of the inadequate security architecture and the faulty concept of data management...

Conclusion:

- Major governmental IT project that practically failed but is still being pushed
- Promises about the scope of services, its scheduling, cost savings and privacy not kept
- Ignorance concerning criticism of IT experts and privacy activists

Source:
http://www.heise.de/tp/r4/artikel/29/29895/1.html
http://www.heise.de/newsticker/meldung/Elektronische-Gesundheitskarte-Zwangsmassnahme-E-Card-21-1135915.html

4.4. The new Schengen Information System SIS-II

Crime scene:

European Union

Time of the crime:

2001 to 2010

Victims:

Every citizen of the EU

Report:

Another example is the major European project to restart the Schengen Information System SIS-II.

In 2001, political will was manifested that the former SIS information system should be developed into an EU-wide instrument for manhunt and data information. These measurements were announced as indispensable. So, in 2004, the order to do so was given to an international consortium of IT engineering enterprises.

Germany's federal government amounted the cost to be expected to around 14,6 million Euro, estimated completion date was 2006.

Briefly: After various setbacks, glitches and problems, SIS-II was declared unnecessary in 2009, three years after the aimed-at completion date of 2006 because contrary to previous statements the hitherto used SIS system was now said to still be capable of development.

In spite of this, the EU commission in charge did not plan to cancel their SIS-II plans. Finally, by the end of October, 2010, the EU parliament pulled the emergency break and the tap was turned off. For the year 2011 alone, there has been an estimated cost of 30 millions of Euros, with a further 90 millions to follow until 2013.

Concerns of human-rights activists, the arguable treatment of the SIS-II-treaty as an international contract and vast privacy concerns on SIS shall remain unmentioned here.

Conclusion:

- Failing of an ambitious European IT project
- Misjudgement of technical requirements and cost
- Inability to break up the project by the time
- (Furthermore, the violation of the European convention of human rights)

Source:
http://www.heise.de/tp/r4/artikel/32/32490/1.html
http://www.heise.de/newsticker/meldung/EU-Parlament-dreht-SIS-II-den-Geldhahn-zu-1122320.html

5. Summary and Conclusion

Summary

- Data cannot be secured – misuse happens on a daily basis
- Incidents usually don't reach the public

Conclusion

Distribution and longevity of digitized data cannot be mastered. Therefore, they are a very grave risk for survival and further development of democratic social structures.

Compressed storing of sensitive data is highly negligent.

Data minimization and the avoidance of concentrated and unified information have to develop into an indispensable imperative of governmental action.

Democracy is characterized by renunciation of information.

(Spiros Simitis, 2009)

6. Glossary

Accesspoint …..... Component providing a wireless network or enabling connection to a physical network.

Accounts …..... User data needed to login to a service or system.

Administrator …..... Person responsible for the maintenance of a local network of computer systems, servers and software, usually having access to all data and system specifications within that network.

Browser …..... Software for downloading and displaying websites.

BZSt …..... (German) Central Federal Tax Agency / Bundeszentralamt für Steuern.

Compliance …..... Acting according to guidelines or legal precepts.

Data Mining …..... Trying to detect patterns in data sets by applying statistical/mathematical methods.

Database …..... Application or system for the structured storage of large amounts of data.

Terminal systems..... Within a corporate network, there are usually different systems at work:

- Central systems for storage and processing of server data (backend systems, e.g. databases)
- Central systems for connecting users (frontend systems, e.g. web servers)
- User systems (end/terminal systems), usually desktop computers, laptops or terminals.

File server …..... Central computer for data storage

Frontend …..... Interfaces or systems within the user's view and reach. These systems may fall back upon so-called backend systems invisible to the user where the actual data are stored.

Hardening …..... Process of securing an IT system against attacks.

IT …..... Information technology, comprising computer industry as well as technology services.

Keylogger …..... Piece of software or hardware designated to protocol, monitor and reproduce ((trace back)) computer keyboard input.

Pentest …..... (Short for penetration test) Security test to identify weak spots within a network by simulating an attack. During an off site pentest, the network is attacked from without, e.g. via the internet. An on site pentest uses network access from within the target's physical structures.

Phishing …..... Method of tricking people into sharing their passwords or other bits of information. This is achieved by setting up a fake website that prompts the input of user names and passwords and saves these data for unauthorised third parties.

PNR …..... Passenger name records, personal data of air travellers (the USA demand detailed data on every person entering the country).

Policy …..... Guideline, instruction of binding character

Provider …..... Supplier of internet access, webspace, e-mail- or telecommunications services.

RFID …..... Radio frequency identification, contactless system of transmitting information via radio waves. The data on an RFID memory chip (as in cards or label stickers) are read out contactlessly using a reader device's radio waves. Depending on system and signal strength, the distance required between chip and reader ranges from few millimeters to several metres. RFID is employed in access systems, warehouse price labels, in the new German ID card and in the passports of various European states.

Scoring …..... Risk evaluation by combining statistical data with empirical facts and assumptions. A well-known example is the assessment of a person's creditworthiness based on his/her residential area.

SIS …..... Schengen Information System, non-public database for people and things under search warrant, disallowed to enter or known to be missing in the Schengen Area.

Social Engineering .. Interpersonal manipulation of people with the aim of unauthorized access to information, data or things. A typical example would be a phone call to an employee, pretending to be a new colleague and requiring the personal password for urgend maintenance work.

SQL-Injection …..... Attack during which, by entering certain command sets on an input mask (e.g. on a website), one may gain direct access to the databases in the background.

Switch …..... Distributing component in a network

Trojan, Trojan Horse Program that's passed on to another computer user under pretext or hidden within another program, designed to gain control over the targeted system.

VLAN …..... Virtual Local Area Network, technology for the virtual separation of actual physical networks into subsets of smaller networks or security areas.

Data Retention …..... Storage of connection data for all telephone and internet communications, not requiring any actual previous suspicion.

Whistleblowing …... Revelations of a usually dicey or controversial nature, being published for mostly selfless reasons. Often a whistleblower puts his own professional existence at risk, if not his life. Web platforms such as Wikileaks have been founded to give whistleblowers the chance to publish anonymously.

WLAN …..... Wireless Local Area Network, wireless technology to connect computers (notably laptops) to the local area or corporate network or to the internet.

7. Imprint

Publisher:

Arbeitskreis Vorratsdatenspeicherung, Deutschland
/// (German Working Group on Data Retention) ///
www.vorratsdatenspeicherung.de

Authors, contributors:

A couple of fine people from „AK Vorrat“
Amongst others: Pgamerx, JRS, Frank-DSR, Wurzellicht, Axel, Kasia, Roam, Vera, Freak, cwoehrl, Gero, Micha

Concept, responsible according to press law:

Michael Ebeling, Kochstrase 6, 30451 Hannover, Germany,
micha_ebeling@mail36.net

Arbeitskreis Vorratsdatenspeicherung
www.vorratsdatenspeicherung.de