Internationally Conference on IT-Incident management and IT-Forensics

IT based crime: Evidence Collection and Legally Restrictions in Investigation Cases

Senior prosecutor Jens Gruhl, Constance

Stuttgart, September 12, 2007

1 Computer Crime

Computer crime is nothing new. The police criminal statistics of the past years have shown high values of the computer crime over and over again. However, it concerned the improper use of Eurocheque cards - a classical case of the computer fraud after section 263a of the German Criminal Code. Such actions are not an occasion for conferences like today.

The limitless Internet has shifted the main focus not only in Germany. Every offender can commit everywhere in the world with e-mail{email} and World Wide the web criminal offences.

The political leaders of the states in Europe have recognised this. On the 23rd November, 2001 the member states of the Council of Europe - not only the European Union - have signed the Convention on Cybercrime. The Convention become effective on the 01st July, 2004. Indeed, Germany has signed the Convention, but has ratified not yet. The German criminal law nevertheless contains some regulations which allow a pursuit of the computer crime.

1.1 Computer Crime in the Real Sense

There is not a legal definition in Germany. However, single sections refer to electronic dates or data processing systems. It concerns :

- Computer fraud
- Falsification of proof-considerable data
- Data alternation, computer sabotage
- spying out dates
- Software piracy
- Producing, leaving, spreading or getting so-called „ hacker tool “ which are invested on unlawful purposes

The Cybercrime Convention contains following definition :

- „computer system" means any device or a group of interconnected or related devices, one or more of which, pursuant to a program, performs automatic processing of data;

- “computer data” means any representation of facts, information or concepts in a form suitable for processing in a computer system, including a program suitable to cause a computer system to perform a function.

1.2 Computer as Action Tools

All offences with which the electronic data processing is used for the planning, preparation or execution belong to the computer crime further. For example, the so-called Ebay deception can be committed only by means of computer and Internet.

In the end, a personal injury which was committed with a keyboard would be also to be added. However, such criminal offences are not the problem of the today's conference.

2 Phishing

In computing, phishing is a criminal activity using social engineering techniques. Phishers attempt to fraudulently acquire sensitive information, such as usernames, passwords and credit card details, by masquerading as a trustworthy entity in an electronic communication.

According to an investigation by BITKOM (press release from the 29th August, 2007) offenders removed in 2006 approximately 13 million euros of the accounts of the victims in more than 3,250 cases. For 2007 an increase is expected once more about 25%.

Phishing seems to be with a damage of only 13 million euros no problem. Account holders suffer on average "only" losses in the lower 4-figure range.

Phishing is nevertheless a problem in varied regards.

2.1 Manifestation

The offender send to the potential victim email officially. The victim should inform the offender of important information (passwords, access dates for online banking, for mail-order firms, Internet auctioneers, web-based online consultations or contact portals) . With the "stolen" access dates the offender can take up performances under wrong identity or effect product dealings. As far as PIN / TAN informations were attained, the offender can arange bank movements immediately.

To wake the appearance, e-mail come from a certain company, the offenders use e-mail-adresses who are similar to those of the well known companies. The offenders use logos and brand names of the affected companies. Sender specifications are falsified. The computers which were "captured" within the scope of so-called bot-net are also used.

From juridical view different sections of the penal code are relevant:

- Production of a „fake“ web page of a bank or similar, plentiful dispatch of emails to a huge number of e-mail addresses (spam),
- Input of the access dates, as a rule, account number and PIN / TAN of a bank account on a web page by the entitled bank customer who feels requested by his bank ,
- Use of the account access dates for the transfer on the account of a domestic person involved,

- Transfer about western union abroad.
- The number of the offenders is uncertain. A single offender can commit all parts successively.

2.2 Applicable Penal Code

The mentioned phases of the Phishing are controversial from juridical view in detail. One affirms basically a liability to penalty of the involved offenders.

2.2.1 Bulding a web page, dispatch of e-mails

Preparation of a computer fraud (Section 263a paragraph 3 Criminal Code): faked web sites do not count as computer programs. This section is not given.

Falsification of proof-considerable dates (Section 269 paragraph 1 Criminal Code): The e-mail informations emails are falsified in the spam emails. Because the legal relations (still) trust in the genuineness, these dates might have enough relevance. This section can be applied.

Spy out from dates (Section 202a paragraph 1 Criminal Code): The injured person gives administer the dates himself. The section is not fulfilled.

Computer fraud (Section 263 a Criminal Code): Then the dispatch of e-mail would have to be looked as a beginning of the action, not (only) as a preparation. By the dispatch the spam email the dispatcher does not know the consignee. A huge number of the messages also goes to the emptiness. Because the action of the victim is inserted, the mail dispatch can be evaluated for this only as - not punishable - preparation action.

Deception (Section 263 paragraph 1 Criminal Code): The mailing should move the consignees to the revelation of the account informations. From view of the offenders everything is already done to cause this success. As an attempt of a deception this can be evaluated if the revelation of the account informations (PIN / TAN) leads at least to a lost of money. The offender can load the account without big{great} trouble with booking entries. Therefore this action is considered as a deception in the district of the general public prosecutor's office of Karlsruhe.

Trade mark right offence (Section 143 paragraph 1 Trademark Act): The offenders use logos and brands which are protected by law. However, requirement for a liability to penalty is that the offender acts for gain. This is given, because the offender does not act as a private individual or as an authority.Therefore, the offender's action is according to the Trademark Act punishable.

2.2.2 Input of the Dates

The erring account holder is not punishable. Civil liability questions remain disregarded here.

2.2.3 Abuse of the Access Dates

The offender uses the dates unauthorizedly. The transaction to costs of the bank customer fulfils the elements of an offence **of the computer fraud (Section 263a paragraph 1 Criminal Codes)**.

If the offenders act as a part of a gang, the penalty is up to 10 years of term imprisonment.

2.2.4 Transmission of the Money by so Called Financial Agents

With the forwarding of the money persons are commissioned who are residents and do not work with the offenders in a gang. As far as the financial agents

- are credulous, they are not punished.
- frivolously take part (to receive a commission) in the forwarding of the money which comes from a criminal offence, **money-laundering** is considered **after Section 261 Criminal Code**.
- help deliberately the offender in the protection of the money by forwarding, **assistance** is considered **to the computer fraud (Sections 263a, 27 Criminal Codes)** (according local court Hamm).
- act to gain a commission, an offence is considered after **Section 54 German Banking transaction's act**. Forwarding of money shows a financial service which is liable to permission. The exercise without permission is punishable. The action can be also committed negligently.

3 Determination of the Facts

Considerable determination problems bring the phases 1 and 4 with themselves, because they take place (only abroad and the offenders are unknown.

The evaluation criteria correspond to the criteria of the court.

For the German procedural criminal law the principle of the respect for the law is essential. With - as it is expressed in Section 170 paragraph 1 criminal procedure - „to satisfactory occasion “ is to be sued. With the forecast an evaluation of the available evidences is necessary. The evaluation criteria correspond to the criteria of the court.The evidences to be presented to the court have to go legal-compliant attained and usably.

The allowed measures of the law enforcement agency are enumerated in the criminal procedure finally. Basic is the right of the law enforcement agency to be able to browse with judicial decision a dwelling house or office rooms .Evidences as well as assets can be seized.

3.1 Phisher

It is obvious that the offenders who operate in the distance are hard to be determined. In addition they appear not personally, but only electronically.

Indeed, the transaction is stored at the bank. These dates can be traced back. Essential track is the IP number.

However, problems arise,

- if the action a long or also short time dates back,
- information to IP numbers is not stored or is deleted,
- the track goes abroad .

Oonly in few cases Phisher were tracked down. About that the press has also reported.

3.2 Financial Agent

The financial agent resident living in Germany is simple to investigate. His account is used for the transfer. About the account number he can be easily identified.

The public prosecutor's office also has the necessary tools to be able to operate fast and efficiently:

- comprehensive clarification of the financial situation by information of the banks
- Examination of witnesses, also by force
- Search with the offender (financial agent)
- Search with other persons
- Seizure of documents and computers; as a substitute also from dates of external computers (LAN, WAN, webspace)
- if necessary: Arrest
- Profit absorption (legal estate seizure)

4 IT-Forensics

If criminal offences were committed with computers, many questions arise.

It is obvious that specialists are necessary.

The police in Baden-Wurttemberg has created special troops. They are quick and efficient to work.

With special questions external experts are also consulted.

Besides, the questions are always the same ones.

- How did the attacker receive access to the network?
- Where did the offender stay?
- Who has carried out the attack?
- What was the destination of the attacker?
- Which changes in the system were carried out?

A problem is that the injured party - unconsciously - can destroy tracks. The attack cannot be further observed. Measures for the protection change the original system. The proof of the action becomes difficult.

4.1 Determinations in Data Networks

Regardless of concrete determinations the Internet is investigated. Problem fields are child pornography, extremism and terrorism.

Importantly to the pursuit are sufficient tracks. In the Internet are this the connection dates. These are stored in log files which are reproached nowadays only few days.

Up to shortening of the memory period by Deutsche Telekom of 90 days for 7 days - what is law-compliant - IP number could become to the track followed.

Nowadays the determinations which lead on the Internet are difficult.

The announced stock dates storage which is measured with six months will bring remedy.

4.2 Determinations in Local Computers

The determinations are easier if a computer (or other system) was seized. The seizure with judicial decision follows if necessary after a search. The legal situation is unequivocal.

The police evaluates the computers. The known technics and software are used.

But also here the first problem fields show themselves:

- access barriers
- encryption of the dates
- big memory sizes
- networked systems which are not fit to work locally any more.

5 Legal Questions with Private Investigations

In the police statistics some computercrime cases are recorded. However, there are many actions which do not become known. There are also actions which are known only the people involved, but not the authorities. Reasons for a non-display can be:

- supposed image and trust loss while becoming known in the general public.
- relatively slightly distinctive interest in a criminal prosecution; civil claims stand in the foreground.
- Companies prefer possibly to sanction own employees as an offender independently without intercalation of the law enforcement agencies.
- no trust in the professional knowledge and skill of the law enforcement agencies.
- one sees no violation of own rights or own legal estate.

In the clarification of the actions big interest nevertheless exists. Experts of the IT-Forensic take action here.

First of all is to be pointed out to the fact that there is not a duty to indicate any criminal offence. It depends on the fact which position one has and which criminal offence is it:

- Police officer must indicate criminal offences from those they get to know occupationally.
- For state employee beyond the range of the criminal prosecution exists no general duty to indicate any criminal offences.
- Private individuals must not indicate criminal offences.

Exceptions:

- Everybody must indicate heavy criminal offences. Section 138 Criminal Code does not concern the classical IT offences (spying out by dates, data alternation, computer sabotage, copyright offences) or child pornography, but:
- Preparation of an attack war, treason, monetary forgery facts, manslaughter, murder and genocide, kidnapping, abduction, extortionate kidnapping, taking of hostages, predatory offences and extortion offences, common-dangerous criminal offences, the formation of a terrorist union.
- Consignees of the indication are an authority or the threatened.

The Indication must follow before the action, as long as the execution or the success can be still turned away.

5.1 Private Investigation

"Private investigation" and the determinations of the law enforcement agencies have the destination to clear up circumstances and as can be proved.

Law enforcement agencies must also clear up exculpatory circumstances. Therefore, the public prosecutor's office cannot delegate the determinations to the injured person or to a private-sector company. The law enforcement agencies accept tips of the injured people any time.

In contrast to the law enforcement agencies private investigators are not bound basically to the rules of the criminal procedure (for example participation of the defender). Also private investigators must not teach the culprit of his rights. Even a deceit as a forbidden examination method is possible.

Private investigators can allow other persons to listen to telephone calls.

However, the law enforcement agencies may not use of such proofs.

Private investigators have, in the end, a big projection. They can take action abroad. They need no registration.

5.2 Liability to Penalty of the "White" Hacker

International agreements like the Cybercrime Convention and the EU- decision No. 2005 / 222 / JI (justice / Internal) from the 24th February, 2005 make the signatories adapt their national criminal law. In Germany sanctions against computer crimealready existed for some years. Possible liability to penalty gaps and these contracts have led to aggravations of the valid regulations and to new sections. The 41-st criminal law amendment act to the fight of the computer crime, dated 8th August, 2007 (federal law gazette, part I, p. 1786 in 2007, published in the 10th August, 2007, efficiently since 11th August, 2007) contains no regulation which makes a punishable the Phishing offence.

Now changed Section 202a Criminal Code also makes a punishable offence the (bare) penetration in a strange, anyhow saved computer - in any case the person does it unauthorizedly. The excuse, one wants to uncover only security gaps, does not drag any more. Without any problems the hacking with order or contract of the owner of the computer remains allowed.

Section 202c Criminal Code is new: he makes a punishable offence preparing the spying out and interception of dates. It is discussed whether the bare possession of malware can be punishable. The section reads (excerpt): "Who prepares a criminal offence after Section 202a or Section 202b, while he produces, sells or another got, leaves to another, spreads or makes usually accessible computer programs whose purpose is the celebration of such an action, is punished with term imprisonment up to one year or with fine."

The new section makes a punishable offence the practise to offer hacker's tools under the coat of the reporting or research only for illegal purpose.

The reporting is made a punishable offence, without this would be necessary.

However, in many cases it does not come to that. Many "tools" can serve several purposes.

The purpose of a program must be determined outgoing by the default of the Cybercrime Convention on the basis of criteria. The miss-use is vital. If a software can be used for preparation actions liable to persecution as well as for legitimate purposes, must be checked which of the ranges of application predominates. Also the concrete purpose (professional application within the scope of an investigation order) must be taken into consideration. The computer programs whose possible misuse liable to persecution is only an unintentional side effect can be used so further.

Final clearness will bring only the jurisprudence.

In any case, the bare possession of hacker's tools is not punishable.

6 Problems with Determinations by Law Enforcement Agencies

Over and over again one hears or speaks from problems which have the law enforcement agencies. Besides, being absent means (money, staff) or the time are often meant. The law position is sometimes deplored, although the constitution binds the law enforcement agencies to the given law. Wishes and hopes should play no role. The politicians lead this discussion.

Nevertheless there are legal restrictions. Determinations or the enforcement of the rights of the injured people are thereby often complicated.

6.1 International Judicial Assistance

Sign of the IT crime is that the stay of offender and victim, the action or the entry of a damage are bound not to certain places, but rather "world wide" take place.

However, also with online actions the competence of German authorities is given, if

- the site of crime lies in Germany,
- the offender is a German,
- the victim is a German or
- the fact that world right principle finds application (par example child pornography).

With foreign relation national measures are allowed only under use of the judicial assistance; with determinations abroad apply the general regulations. "Reliefs" for IT determinations are few and far between.

The Ministerial Conference of the G-8 Countries on Combating Transnational Organized Crime (Moscow, October 19- 20,1999) has decided Principles on Transborder Access to Stored Computer Data and Acessing Data Stored in a Foreign State (excerpt):

> 1. Each State shall ensure its ability to secure rapid preservation of data that is stored in a computer system.
>
> 2. A State may request another State to secure rapid preservation of data stored in a computer system located in that other State.
>
> 3. The requested State shall take all appropriate means, in accordance with its national law, to preserve such data expeditiously.
>
> 4. The requested State shall, in accordance with its national law, execute the request as expeditiously as possible.

5. Each State shall, in appropriate circumstances, accept and respond to legal assistance requests made under these Principles by expedited but reliable means of communications, including voice, fax or e-mail, with written confirmation to follow where required.

6. A State need not obtain authorization from another State for the purpose of:

a) accessing publicly available (open source) data, regardless of where the data is geographically located

b) accessing, searching, copying, or seizing data stored in a computer system located in another State, if acting in accordance with the lawful and voluntary consent of a person who has the lawful authority to disclose to it that data.

In practice the quick conversion fails because of many things. There are language barriers. The law enforcement agencies are often informed too late. The penal provisions are still different in the single states. Besides, different pursuit principles exist.

In practice the quick conversion fails because of many things. There are language barriers. The law enforcement agencies are often informed too late. The penal provisions are still different in the single states. Besides, different pursuit principles exist.

The principle of the obligation to the law („Legalitätsprinzip“) in Germany demands investigations also with small amounts of damage. Par example: The lawyers of originators refund massively displays against the users filesharing- systems.

On the other hand the law enforcement agencies of other states can decide at its own discretion whether they proceed against a criminal offender . Thus a Dutch public prosecutor could also refrain by a deception more than 70,000 euros of determinations. The situation in France is similar.

6.2 Cyber Crime Convention

The Cybercrime Convention (Convention on Cybercrime, CETS No. 185, signed by Germany Sept. 21, 2001, in Budapest) displays an other step on cross-border determinations. Indeed, it is no national German law. However, it is transformed by more and more states.

In their worth reading preamble the states of the Council of Europe have mentioned the destinations. Beside a better criminal prosecution the rights of the citizens should be also protected also against state measures.

The Cybercrime Convention determines in the single articles what the signatories must transform. Beside the fight of the "classical" computer crime the child pornography and offence against the copyright are mentioned.

6.3 View: Online Search

Before the turn of the millennium Orwell's monitoring state "1984" was a threat which was absolutely taken seriously. Data protection and security were a high property good

However, the terror attacks committed in the USA on the 11th September, 2001 have led to a new or at least advanced definition of the term Terrorism. Thus computer crime can be also looked as a terrorist act. Not only in the USA it is conceivable to carry out supervision of the telecommunication without approval of a judge or to

collect DNA-fingerprints from computer criminal offenders and to store them like those from murderers or kidnappers.

After applicable law the law enforcement agencies can carry out searches of flats. Computers in Germany can be seized easily (only the analysis is time-luxurious). Also on so-called anonymization servers can be accessed (Regional Court Constance, MMR 2007, p. 193). An offender can be arrested. The telecommunication can be supervised on a real-time basis. In addition determination possibilities are available like the application of concealed investigators, the search for wanted persons, the post seizure and the living space monitoring.

Legally is not regulated an online search which is carried out concealedly (Trojan horse / Remote control, Keylogger). The introduction is in the discussion (see draft bill of the Federal Criminal Police Office law of the "defence of dangers of the international terrorism“). Computer far away should be browsed on contents. Technical and juridical details are controversial.

Technically the online search as a Trojan horse can hollow out the IT security. The abuse of the technologies by unauthorized is possible (by employees, foreign intelligence, criminals). The up to now known measures do not fulfil the requirements which are put to a court-steady hearing of evidence. At most a hardware solution (Keylogger) could be understood.

The defence of the terror is important. However, the constitution also protects the rights of all citizens.

Some questions are open: Which suspicion degree must be given (beginning suspicion, enough or urgent action suspicion)? How heavy must be the action (range of punishment or concrete debt reproach, " not unimportant ")? Who may order the measure (judge's reservation)? What ist the real Purpose: Danger defence or Secret Service or criminal prosecution?

7 View

Ritsch & Renn’s Cartoon as seen here:
http://www.heise.de/ct/schlagseite/06/20/gross.jpg
("Hello. I come from the German Bank. Chiselers try again and again to attain account information. The newest trick is that people, who aren’t aparently bank employees, go from door to door, in order to spy account data. Therefore we had to change your accounts. Please give me all your passbooks. We will update these for you free of charge.")

To the author:

Senior public prosecutor (Permanent Representative of the leading senior public prosecutor) with the public prosecutor's office Konstanz. Director of a determination department (concerning drugs and organized crimes, money laundering corruption, falsification of money, offences against the war weapon control law). Director of the execution of a sentence department. Press speaker.

Since 1986 in the law service of the country Baden- Wuerttemberg as a judge and a public prosecutor.

1992 - 1995 chairmen judge at the regional court Leipzig.

2001 - 2004 director of the desk for organization in the Ministry of Justice Baden- Wuerttemberg.

Author of legal essays concerning white-collar crime and computer criminality.