Investigations and Prosecution in cases of Computer Crime – Overview of the National and International situation

KOR Fred-Mario Silberbach

Bundeskriminalamt (BKA)
SO43 Analysis, Investigations, High-Tech-/
Computer Crime, Random Internet Searches
65173 Wiesbaden, Germany
fredmario.silberbach@bka.bund.de
so43@bka.bund.de

1. Crime Statistics and Developments / Trends

Regarding the Crime Statistics (Polizeiliche Kriminal-Statistik - PKS)[1], which is published annualy by the Federal Criminal Police Office (Bundeskriminalamt – BKA), could lead to the following conclusion: The real situation of Computer Crime is not very clear.

The definition for Cybercrime, which is written down in the Cybercrime Convention of the European Council, still has not been ratified by Germany. So there is still no legal definition for computer related crime in Germany.

For a better understanding about the statistics concerning computer crime it is necessary to point out that the national crime statistics of the BKA differentiates between

- Computer Crime in a so-called common sense, that contains all crimes where the Internet was used as an instrument for committing the crime and
- Computer Crime in a so-called closer sense, that contains offences like Computer Fraud, fraud by accessing communication services, forgery of evidentially data, data espionage, alteration or sabotage of data and computer sabotage.

In 2007, in Germany 179.026 crimes were reported to the BKA where the Internet was used – in a common sense - as an instrument of crime. This means an increase of 8 % compared to 2006 (165.720). 73% of all reported crimes were fraud offences and 40% of the total number of these offences (71.876) concerned fraud by obtaining goods.

The number of computer crimes in a closer sense has risen from 29.155 in 2006 up to 34.200 crimes in 2007, which is an increase of about 17,3%[2]. A further rise in the next years must be expected.

Phishing is not a crime which is officially listed in the German Penal Code. Phishing describes a modus operandi which consists regularly of the listed crimes data espionage, data alteration, computer fraud, obtaining goods by fraud and money laundering. Therefore, the numbers of Phishing cases are also not listed in the above mentioned National Crime Statistic.

[1] Bundeskriminalamt, 2007, Polizeiliche Kriminalstatistik, p. 236, Wiesbaden/Germany
[2] see above

To get an impact about these numbers it is necessary to evaluate the criminal cases which are reported by the Criminal Investigations Departments on an additional Case Reporting System.

Concerning Phishing in connection with online banking, in 2006 3.500 cases were reported to the BKA with an average loss between 2000 and 3000 € (total loss between 7,000.000 and 10,500.000 €). In 2007, already 4.200 cases were reported with an average loss of 4.500 €[3] which means a total loss of 19,300.000 €. But not every case has been reported to the BKA and a considerable higher number of cases and a higher loss must be estimated - only in 2007 and only in Germany.

At the end of 2007 and the beginning of 2008 in Germany also the last of the big German bank corporations implemented the iTan (individual Transaction-Number), an updated and saver mechanism for online banking instead of the PIN/TAN-method. The positive result: In the first seven months of 2008 the number of Phishing cases decreased to 1.100 cases which means a reduction of about 54% [4]. But now the BKA notices a higher intensity of attacks against banks which are using the iTAN-method. Actually there exist at least three Trojan-Families which attack the in Germany commonly used iTAN-method. One of these families focuses only the German Market and attacks exclusively German banks. And mostly, this modern malware is not detected by signature-based antivirus-software.

In the last years, the offenders could catch credit or debit card data, ebay or banking account information because the computer users – the prospectively victims - clicked on links in received Emails and entered their login data at faked websites. But the situation has changed. Phishing via Spoof- and Fakesites has nearly vanished in Germany and throughout large parts of Europe. Malware is hitting the market massively. 99% of the Phishing cases reported to the BKA now is being done by malware. Partly, this malware still is downloaded to a computer because the user opened an attachment. But the development shows an increasing rate of drive-by-infections, that means, when users follow a link to an infected homepage or when users only visit infected homepages from innocent companies, restaurants and internet-services. This modern malware is evolving quickly and aiming for multi-usage business models. It is self-upgrading, built-on-demand, it does contain not only Keylogging- and "Man-In-The-Middle"-functionalities but also Proxy-, Remote- and Spam-capabilities.

In an investigation of the BKA, in September 2007 a group of 10 offenders was arrested, which had caused a loss with trojan-based Phishing of nearly 700.000 € in a period of 18 months.

But Phishing is not limited to banks anymore. Malware, infected computers and networks can be used in more than one way to generate money. Phishing now is about losing the digital identity in its entirety. This contains e.g. the access to Email-Boxes, to ones company network and/or distributed resources, to online merchandising services (e.g. ebay, amazon) and to social networking portals (e.g. stayfriends.de, xing.com).

[3] Bundeskriminalamt, 2008, Kriminalpolizeilicher Meldedienst – KPMD, Wiesbaden
[4] see above

Stealing data of credit cards becomes more and more popular. In 2007, the online-gaming portal „Steam“ was successfully compromised and millions of valid sets of credit card-data had gone lost. Rumours are talking of more than 10.000.000 sets of credit card data. Only six hours after this security breach, more than one million of those credit card data-sets were offered in the so called Underground Economy by specialised resellers. In another case of 2007, a company lost 45.700.000 datasets of valid credit and debit cards.
These just mentioned cases are only two examples among many others. As direct consequences, many banks and/or online merchants worldwide are being hit by fraudulent transactions pointing back to those incidents.

Stolen data are sold and bought in the just mentioned Underground Economy. For example, datasets of German credit cards with a limit of 5000 € are sold for 2€ each, US-cards are sold for only 1 € - and an additional discount for buying great numbers of datasets is also possible.
The Underground Economy is furthermore a global market where services around digital identities are traded. And the amount of stolen data is searched and filtered by special software (“Harvester”) to generate single information that can be used by special interested offenders to commit other crimes. Today, it is absolutely no problem to find, to hire or to buy components or services like malware, financial agents, spam sending services, anonymized or encrypted communication channels, false identities, credit card data, login / access data for all sorts of digital identities, anonymized internet based payment-systems, which also can be used for money-laundering, and exchange offices for digital currencies.
Knowledge and resources are traded and paid with digital currencies like E-Gold and Web-Money.

In spite of all the above mentioned data, information and examples, a considerable dark field must be assumed. Regarding present hints, a successful invasion of a computer very often is not noticed by the user or owner. And especially in those many cases of noticed attempted invasions or completed invasions but without financial loss, the user do not complain the attack to the police. Last but not least, attacked companies regularly do not report attempted attacks or successful invasion to the police. The reasons might be the expected and feared loss of reputation, the confidence among their private and commercial customers and also questions of liability.

2. General Conditions for investigations and prosecution of Computer Crime in Germany

The “typical user”
Due to statistics of the Federal Statistical Office, in 2007 round about 28,300.000 Computers (PC, Notebooks, PDA´s) were used in private households[5]. A lot of these computers are bought by “normal users” in department stores, in internet-stores or internet-auctions and also in discounter stores. In most cases these computers are equipped with a timely limited security software or only with test- or beta-software-versions. In many of our known cases the victims were using the computer for surfing in the internet, for doing online-banking, for chatting, for changing files and for all the other interesting things – but without any or a sufficient protection of their computer. Very often there is still no or not sufficient knowledge about the risks of using the internet and the possibilities to protect the computer effectively. And also users with an increasing or outstanding knowledge

[5] Statistisches Bundesamt – Destatis, 2008, Wiesbaden

about risks and measures become more and more victims because the offenders develop new and very professional malware and techniques to steal data and information.

Darkfield Economy

A base for developing strategies and measures to fight against crime are the statistics about reported crimes. Of course, sometimes the validity of those information is limited and it has to be added by estimates or results of research to get further information about the dark field and to get an impact about the real situation of a phenomenon.
But concerning the situation of computer crime in the German economy it must be noticed: it is very dark! The BKA just has little information about quantity and the quality of computer crimes that are committed against economic companies in Germany and also about the caused loss. This dark field „Economy" makes it nearly impossible to estimate the real situation of computer crime, to develop strategies and enforce measures against those crimes and also to advise the politics. It is obvious for everybody: to reach a target or to fight against an enemy it is necessary to see the target or to know the enemy.

Legal possibilities and limits

Other important aspects are the legal possibilities and limits for investigations in cases of computer crime.

In March 2008 the German Constitutional Court has confirmed in a preliminary decision the general obligation for the suppliers of telecommunication services to preserve traffic data so that the police or other authorities can demand and collect those data in cases of serious crime. But from the point of view of the High Tech Crime Unit of the BKA it is necessary, that the Constitutional Court confirms the legitimacy of the complete regulations of the specific rule.
For starting investigations and to solve cases of computer crime the existence of traffic data is essential. Without any traffic data, in many cases it is useless to start the investigation and the file has to be closed directly after a case has become known to the police. When e.g. hackers attack the server of a company to steal sensible information, the IP-address at the moment of the attack regularly is the only starting point for further investigations. In these many cases of Phishing, the IP-addresses of the offenders – except the bank account data of the financial agents in Germany - are the essential information just to start and to move one step closer to the offender.

A long period of time, the internet service providers were not liable but also not yet authorized to preserve traffic data.
Due to Directive 2006/24/EC of the European Parliament and of the Council on the "Retention of data generated or processed in connection with the provision of publicly available electronic communication services" (March 2006), the supplier of telecommunication services in Germany have to preserve traffic data for a period of six months. Several times not only the BKA has demanded this result of an European agreement which – by the way – in Germany stays 18 months under the period of maximum 24 months which is allowed by the above mentioned European directive.

In this context it is very important to point out, that the preservation of traffic data is not only necessary to clear up crimes – it is also necessary to avoid crimes or to prevent danger in general.

At the end of 2007 there was a case, while in a running chatroom session in Germany a person had announced a run of amuck. The lack of stored IP-address-data here but the knowledge about an Email-account hosted in a foreign country was the only way to get more information in this situation. Due to the lack of further information about the owner of the email account, the foreign National Police Office had to seize the content of this account. They mailed it to Germany and by evaluating the content it was possible to identify the responsible person. The result of many hours of investigating, phoning and mailing during the night and a part of the week-end: The person could be found – but only luckily. In this case, the person did not intend to run amuck in reality. But other announcements – also from people who want to commit suicide - might have a real background. Should it depend only on a lucky chance to clear those situations?

Regarding the task of the police, to fight against crime and to find evidence with different criminalistic methods, the present problems and challenges, based on experiences on different cases investigated by the police, can be described as followed:

Technical development

Doing searches today, the police finds and seizes more and more technical equipment like personal computers, notebooks, PDA´s, mobile phones, digital cameras, mp3-players etc. Computers with a capacity of one terabyte and more are not rarities any more. Only in one case, a seized computer with a hard disk containing 2,5 terabyte of data in 300,000 files had to be evaluated.

Today, offenders communicate regularly with mobile phones, by Voice over IP (VoIP) or via the Internet, very often also using Internet-Cafes, Call-Shops or not-protected WLANs of other people. It must be noticed that offenders save their information, which are evident for the police, increasingly not only on their computer at home but also in the webspace. And it is also not a secret that anonymity and encryption of communication and at the storage of data takes place more and more. The decryption of seized IT-evidence and communication data demands a high personal and technical effort or it is increasingly impossible.

There is an increasing use of broadband internet access with a data transfer rate nearly 2000 times faster than an (old) analogue line. The consequences: Only one interception can block a major part of the interception and data storage capacities of a big Criminal Investigation Department. And these amounts of data also must be verified and evaluated, in general by police officers. But the number of police officers does not increase as much as the amount of data.

Training and Equipment

For doing investigations effectively and with the correct criminalistic and forensic methods, in general well qualified personal and also modern hard- and software is needed.
But do we already have such experienced police officers in every police station or Criminal Investigation Department in the country? Officers, who exactly know what to do when an victim, e.g. in a Phishing case, comes to them to file a complaint? Or in cases, when network administrators, that have noticed unauthorized data traffic in an obviously infected and captured server, want to give the police a little chance to intercept this data traffic in order to find the offenders instead of just stopping any network activity? No, but the police is working on it, although the police has many other duties in order to protect the citizens and to fight against other forms of crime. The police in Germany has recognized this problem and meanwhile founded special High Tech Crime Units at different police

offices – yet mostly at bigger Police or Criminal Investigation Departments. But in the federal structure of Germany the situation between the sixteen National States still is different.

These problems - or challenges - in general also concern the judicial bodies. Single statements of prosecutors and judges and also experiences of investigations showed partly a lack of knowledge about new technologies, a lack of acceptance for new challenges and also a lack of willingness to go new ways for the handling of such cases at court.

3. The International Situation

The just mentioned examples to show the general conditions for investigations and prosecutions in Germany and the hereby following problems for the fight against computer crime become another dimension when the cases become international. And it is obvious, that there are only a few cases or nearly no cases where the perpetration occurs only within the national borders.

In an essential part of the cases of computer crime it is normal to find

- E-Mail-Accounts of offenders at foreign Internet Providers or Mail Services or in Germany offered internet services but where the content of mails is stored on foreign servers
- Malware stored on foreign servers to get downloaded in order to infect or capture computers or networks in Germany
- IP-Adresses from foreign servers when attacks were enforced and noticed
- Foreign servers where stolen data or tools to commit further crimes (e.g. like Rock-Phish) are stored, changed and dealt with.

These are just a few examples to show the international character of Computer Crime. But while enforcing an investigation for the police or the prosecutor it becomes interesting now.

To improve the change of information about E-Mail-Accounts, IP-addresses and other stored data, in 1999 the G8-countries published "Principles On Transborder Access To Stored Computer Data"[6]. Among other things, these principles declare for example, that the different states

- shall ensure their ability to secure rapid preservation of data stored in computer-systems
- may request each other to secure rapid preservation of data stored in such systems
- shall take all appropriate means, in accordance to its national law, to preserve data as expeditiously as possible.
- shall execute requests for expedited legal mutual assistance in accordance to its national law as expeditiously as possible.

To ensure the implementation of those principles, the G8-countries first installed a network consisting of single point of contacts in each country with a 24 hour 7 days a week presence. In Germany, this single point of contact is within the High Tech Crime Unit of

[6] G8 - Ministerial Conference on Combating Transnational Oranized Crime, October 1999, Moscow

the BKA. These G8 24/7 points of contact are provided for investigations involving electronic evidence that require urgent assistance from foreign law enforcement. The introduction of the so-called "preservation order" provides the members of the network with an instrument that helps to freeze volatile data in a target country before an official letter rogatory for data preservations will be sent through the appropriate channels – a process that is time consuming and which normally takes longer than the usual storage of data.

This network has grown during the last years and actually there are similar contact points in 50 countries worldwide. But this shows also, that many countries still don't have installed such units. To communicate with those states in cases of computer crime, it is necessary to use the normal Interpol channels. In general, the communication in such cases needs more time and sometimes it is not clear, if, when or from which foreign unit exactly you will get an answer for your request or not and whether the results justified the efforts before.

To ensure that the information which has been exchanged through appropriate Interpol channels reaches the specialized police units with the least possible delay, Interpol has compiled a list of National Central Reference Points (NCRPs) for computer related crime. To date, nearly 120 National Central Bureaus of Interpol have designated such NCRPs. These NCRPs are also an essential prerequisite for the establishment of an early warning system.

The introduction of the above mentioned measures were important first steps to improve the fight against Computer Crime. But a continued international harmonization of the legal base in the different countries is furthermore necessary.

To receive information from other countries, for example information about the subscriber of IP-addresses in an actual Phishing-case, first of all it is necessary that the crime, that happened in one country and which was the starting point for a request to a foreign country, also is a punishable act with regard to the foreign penal code. Further it is necessary, that the domestic law in the countries regulates e.g. the preservation of traffic data and the obligation for Internet Service Providers to hand out requested information immediately to the police.

As far as these requirements are not met, in many cases of computer-related crime it is even not necessary to send requests to different countries. And also in Germany it is still necessary to answer many countries, that they will not receive a suitable answer to their request concerning traffic data because of the present legal situation at the preservation of traffic data.

4. Needs for Action

To improve the fight against computer crime there are various measures which should be enforced.

It is necessary to establish specialized units at the police offices and to implement specific training programmes. In Germany, the BKA - in cooperation with the State Police Training Institutes – is currently setting up a national training programme for first responders, case officers and IT forensic experts. It is also necessary to think about setting up public

prosecutors offices specialized in IT-crime and to establish specific training not only for law enforcement offices but also for prosecutors and judges.

Concerning the legal bases, a wide spread ratification of the United Nations Cyber Crime Convention is necessary to improve the international cooperation by establishing unique standards in all the member states in the world.

The need and the importance of the preservation of traffic data for the investigation in cases of computer crime already has been described. It now depends on the final decision of the German Constitutional Court to give the police this necessary instrument.

A better and closer cooperation is needed, on an international and a national level, and also between law enforcement offices, IT-based offices, the Internet Economy, banks and other private organizations and institutions.

On the international level there is now a working party of the Council of Europe "Cooperation between Service Providers and Law Enforcement against Cybercrime". It consists of participants from law enforcement offices and the industry and develops common guidelines for the necessary cooperation in the future.

The biennially Interpol conference on Cybercrime is a useful platform to meet the counterparts of the BKA from many other countries, to exchange information about the phenomenon and to develop strategies and measures against this sort of crime.

In Germany a closer cooperation between the BKA and the Federal Office for Information Security[7] on technical issues has been implemented.

It is also necessary to raise the awareness among the public and also among parts of the economy concerning the threat of computer related crimes and the possibilities to react on it.

The "Programm Polizeiliche Kriminalprävention der Länder und des Bundes" (ProPK) is a cooperation between the Federal Gouvernment and the National States in Germany to prevent of crime. Together with the ProPK, the BKA develops and publishes the so called "IT-Newsletter" with information for the people in Germany about new trends and how to minimize their risk of becoming victims of crime.

Very important is a better information exchange – especially with the economy. The police is not the enemy of the economy. But a better information exchange with respect to the respectively needs, possibilities and limits can help the police and the economy to provide a better and safer environment for "their customers". The implementation of a frequently information exchange with representatives from the BKA and several german banks is only one opportunity to go into the right direction.
The participation of different representatives of the economy in a current project group of the german police to develop a common strategy against computer-related crime is another example to improve the national cooperation.

[7] Bundesamt für Sicherheit in der Informationstechnik – BSI

5. Outlook

In the time of a fast developing technology and also of fast developing methods for committing crimes transborder, worldwide and within milliseconds, the society must give the state and his police the necessary instruments to fight against this crime.

Due to the constitution, the state is responsible for the safety of its citizens. The German Constitutional Court (Bundesverfassungsgericht – BVerfG) has emphasized several times the peremptory need for an effective criminal prosecution and for a fight against crime. There is a public interest in a complete - as possible - establishment of the truth. Of course – not at any price. The State has to respect the constitutional rights of its citizens.

There are critics and statements, that the State only wants to collect more data and information to improve the possibilities of observing and intercepting its citizens or to control the whole society. It is also asserted, the State would hurt the constitutional rights of its citizens.
But these critics should compare the fast speed of the technical development and the up to date grown possibilities of fast and worldwide communication in the area of Computer Crime on the one side with the development of the legal possibilities of the State on the other side. And the critics should also take into consideration, that the demand for respecting the constitutional rights of the citizens means also, that the State has to care for those citizens, which have a legitimated claim to get protected by the State.

The president of the BKA, Mr. Ziercke, expressed the willingness of the BKA and the Police of the German National States to carry on an open and fair dialogue based on the intelligence about the situation of crime[8].
With relation to questions directly concerning the phenomenon computer crime, also the High Tech Crime Unit of the BKA is open for dialogues and discussions.

[8] Jörg Ziercke, 2007, „Polizei in der digitalen Welt“, Autumn Conference Bundeskrimimalamt, Wiesbaden