DPT

Deutscher Präventionstag –
der Jahreskongress seit 1995

Cybercrime - the darker side of the digital society

Jörg Ziercke

From: Marc Coester and Erich Marks (Eds.):
International Perspectives of Crime Prevention 7
Contributions from the 8th Annual International Forum 2014
within the German Congress on Crime Prevention
Forum Verlag Godesberg GmbH 2015

978-3-942865-38-8 (Printausgabe)
978-3-942865-39-5 (eBook)

Jörg Ziercke

Cybercrime - the darker side of the digital society

1. Introduction

Ladies and Gentlemen,

Thank you very much for giving me the opportunity to open today‘s special event on Cybersecurity as part of this year‘s German Congress on Crime Prevention.

First some preliminary remarks on the objectives of my presentation.

1. Reports on cybercrime are aimed at clarification, not demonization.
2. Knowledge of cybercrime aims at raising user awareness, protecting the user.
3. Trust in the internet is to be strengthened.

My aim today is to look at prevention, not legal aspects arising from encryption and anonymisation.

The internet has permeated nearly all areas of life; for many it has become an integral part of their lives. “Always on” is the catchphrase. Terms such as “smart home”, “internet of things” or “industry 4.0” are synonyms which underline the fact that modern IT, data processing and the internet will influence our everyday lives and economic activities to an even greater extent in the future.

During the time it took me to give this brief introduction, around the world:

- about 1.3 million videos were watched on Youtube,
- more than 2 million enquiries were googled,
- 6 million Facebook entries were viewed,
- 100,000 twitter messages[1] and over 200 million emails were transmitted, though over 90% of these were SPAM mails.

But like all aspects of life, there is an up and a downside! In order to protect yourself from cybercriminals, you have to know more about the phenomena of cybercrime.

Cybercrime is a new dimension of crime which changes each day. Perpetrators have access to countless potential victims and targets worldwide. The potential risk for the individuals, business enterprises and financial institutions, as well as for the state and its institutions, is considerable and omnipresent. For the perpetrators, the risk of being caught is small compared to the analogue world. Cybercrime’s growth potential is boundless, as

[1] Other sources estimate this number at roughly 300,000

is the potential damage it can wreak. The internet has done away with national borders, which means that there are no criminal-geographic areas in the cyber world. Terrorism and organised crime do not recognise any borders and are constantly growing.

One thing is for certain: the internet and modern means of communication have decisively influenced our communication behaviour and social life. On the one hand, they have found their way into traditional forms of crime, especially in the field of fraud; on the other hand we see the emergence of new forms of crime – forms of crime that would not be possible without the use of modern information and communication technology. In almost all areas of crime, perpetrators avail themselves of sophisticated technology and use the internet as an instrument of crime. Throughout the world, people become the victims of fraud, extortion, property crime, phishing, theft of their digital identity, Scareware, Ransomware, cyber grooming and cyber bullying. They allow themselves to be radicalised and recruited, are duped into believing criminal scams of ostensibly online shops or call centres, unknowingly become part of a botnet, the instrument of modern crime. It is not only citizens who are the victims of cybercrime. Enterprises are also the focus of criminal activities.

The objective is to compromise data, to use the digital identity of someone else for one's own criminal purpose, to access know-how and protected information.

But it is also about attacks on critical infrastructures, states or companies.

All users, but especially companies, must actively address the issue of cybersecurity if we are to meet the challenges posed by cybercrime. According to a security study carried out by Corporate Trust, "Industrial espionage 2012", less than half the companies surveyed had a security management with clear regulations for information protection. And only every fifth company had even defined know-how worthy of protection. Studies have repeatedly demonstrated the reluctance of companies to report attacks. Surveys carried out at chambers of commerce and industry have highlighted the fact that only 20% of companies in Germany lodge a complaint following a cyber attack. This means that undetected crime is at least 5 times higher than the official figures!

Why are such attacks not reported to the police?

- Filling a complaint is too time consuming,
- companies are skeptical that investigation by the authorities will be successful,
- or the companies do not know who to contact within the authorities.

And there is another reason: they fear damage to their reputation. However, as long as enterprises fail to recognise the danger or refuse to report identified attacks, the authorities cannot become active and cannot draw up a comprehensive picture of the threat posed. There have always been cases of victims who for various reasons did not report crimes. Many people are unaware of the fact that they are the victim of a crime, many crimes go undetected!

Data theft is a particularly good example: 2.0 theft is a case of copying, i.e. the stolen data is never removed from where it is stored. The “loss” is frequently only noticed when the damage has already been done, for example, a copyright violation or product piracy.

2. Current Forms of Cybercrime

A brief look at current forms of cybercrime

2.1 Phishing

One of the best known forms of cybercrime is probably phishing in connection with online banking. The number of reported cases has fallen, but is still at between 3000 and 4000 incidents.

In 2012, the number of such cases in Germany fell sharply by 46% to about 3,400 (3,440; 2011:6,422). The number of undetected incidents is unknown. The average loss incurred was around 4000 euro per incident. An explanation for this lies in the fact that, in addition to a greater awareness on the part of the users, in 2012 many German banks improved their security systems, especially with the introduction of the so-called mobile TAN (mTAN) procedure. With the mTAN procedure the transaction number required for authorisation for online transactions is sent to the bank customer‘s mobile telephone. The introduction of this second, independent communication channel improves security. We saw a similar drop in the number of incidents in 2008 when German banks introduced the iTAN procedure throughout Germany. However, in the following year the figures rose again and in 2010 had increased well above the all-time high of 2007. It remains to be seen how long the new security system will be an obstacle to criminals.

The phishing tools used develop at the same pace that security measures are introduced. The procedure used by offenders in the early days, when they sent unsolicited bulk emails in which the recipients were called upon to reveal their online banking access data, is almost a thing of the past. Malware is invariably used. The volume of new malware has increased sharply. Every one to two seconds a new malware programme is created somewhere in the world. In order to circumvent the functionality of virus protection programmes, these are normally only active for a few days and are then replaced by new versions.

Currently, phishers favour the following variations to spread their malware.

1. „Drive-by infection“: Unwitting downloading of malware simply by visiting a website which offenders have compromised.
2. The malware is spread via social networks[2] in which the subsequent victim trusts the offender and then either opens infected attachments in good faith or follows links.
3. “Spear infection” Specific individuals targeted with personalised phishing or infection mails with the aim of infecting the computer or obtaining data required to carry out other actions. One reason for this modus operandi is that many internet users have become increasingly wary of opening anonymous emails. However, they are less cautious if the email is addressed to them personally.

Meanwhile, two thirds of the malware is spread by means of drive-by infections. According to the IT sector[3], each day 13,000 infected websites are uploaded on the internet worldwide[4]. Additionally, hackers target frequently visited websites in an effort to manipulate these websites with a view to spreading the malware much faster and reaching a larger group of users. In this way offenders can, for example, disseminate Trojans which are capable of “interposing” themselves between online banking transactions in order to manipulate transfer details.

In spite of a recent fall in numbers, online banking continues to be one of the main targets. Offenders have already responded to the introduction of the mTAN process and have achieved initial successes.

They go about this in the following way:

1. Using traditional phishing methods attackers extract access data used for online banking.
2. Without the bank customer being aware of this, they then set up the mTAN procedure. The offenders provide a mobile number for receipt of the mTAN.
3. The activation code provided by the bank per mail is intercepted by the offenders.
4. The offenders are now able to transfer money from the bank customer’s account.

But even this scam is now a thing of the past. In the meantime we can see a technically more sophisticated attack scenario. Here the offenders use malware to attack the mTAN procedure on Android smartphones, making it is no longer necessary to infect a computer. The offenders are not only responding to the introduction throughout Germany of the mTAN procedure by the German banks, but also the increasing use of smartphones and tablet computers for online banking.

[2] E.g. Facebook, Studi-VZ, Wer-Kennt-Wen

[3] IT service provider Symantec

[4] dpa press release dated 2 March 2010

This development demonstrates that the offenders are constantly endeavouring to keep pace with security applications on the market. The extent to which the offenders are market oriented is demonstrated by the fact that devices using the Android operating system are attacked. 75% of all mobile terminals worldwide are run on the Android operating system, which means it holds a dominant market position.

- The "Google play store" alone offers almost 1 million apps for this operating system, not to mention apps offered by third parties. There is a real possibility of coming up against a "black sheep", and possibly malware.
- Almost 700,000 malware variations have been identified on Android devices since the beginning of this year.

Many Android devices use even older versions of this operating system. There are usually no support contracts and thus no obligation on the part of the manufacturer to provide updates. The consequences: security vulnerabilities which are identified after a device has been purchased are not fixed. The devices are often poorly protected.

2.2 Digital Identity

Cyber criminals are interested in all types of access data which ultimately enables them to conduct internet transactions at the expense of third parties and for their own benefit. The digital identity is the sum of all possibilities and rights of the individual users and their activities within the overall structure of the internet. In concrete terms: All kinds of user accounts including passwords.[5]

The German authorities are currently dealing with a case where investigations into cyber criminals resulted in the discovery of a data collection of about 16 million German and other e-mail addresses with passwords. It is not yet known how the offenders obtained the data, whether the data has already been fraudulently misused and, if so, what possible losses have been incurred. You have doubtlessly heard that in connection with this the Federal Office for Information Security set up the website "www.sicherheitstest.bsi.de" at the beginning of 2014. Internet users were able to check if data associated with them was listed. Some 30 million people made use of the service. There were about 1.6 million hits directly linked to the requesting parties, i.e. the email in question was amongst the 16 million stolen data files.[6] Recently, another case of 16 to 20 million stolen email account data became known.

[5] Examples: E-mail and messenger services, social networks, e-commerce (online banking, online brokerage, sales portals such as eBay, reservation systems for flights, hotels, etc.), home office accounts with access to internal company resources, e-government, cloud computing

[6] As of 12 February 2014: 29.7 queries, 1.58 million hits

2.3 Carding

Credit card data in particular, including payment addresses and further information, is also a part of one‘s digital identity. Our estimates indicate that over the last few years at least 200,000 credit card holders in Germany were victims of fraudulent credit card transactions – a trend that is on the increase. We are talking here about „carding“.

We estimate that the financial losses incurred by the German financial sector alone were in the mid three-digit million euro range – approximately 70 % of these losses were the result of Internet transactions! According to Interpol, more than 160 million lost credit card data with a purchasing power of over 5 billion USD was recorded throughout the world in 2010 alone.

Let me give you an example of the profitable use of credit card data by cyber criminals:

One of the largest modern-style bank robberies was committed exactly one year ago. Following successful hacking attacks, offenders used forged credit cards to make 17,000 withdrawals totaling about 40 million USD in 23 countries around the world within two days. 2.3 million euro was withdrawn in eight cities in Germany.

2.4 Scareware, Ransomware

A further example of the perpetrators’ inventiveness is the use of what is referred to as Scareware – software that is meant to generate fear. The user is guided onto a web site where he is led to believe that a system scan for viruses, trojans etc, has been conducted on his computer and a large amount of malware identified. The user is then offered a tool to remove the malware. During the execution of the tool on the computer a purported anti-virus solution is installed. This has to be paid for and registered following installation. Because he is concerned about the security of his data, the customer discloses his credit card details for the payment. Whilst providing this data the customer is called upon to supply further information in respect of his address and/or email address. What the customer does not know is that the tool installed for the purpose of helping him avert supposed threats to his computer in fact ensures that malware is installed on his system.

With regard to the number of offences committed using Scareware: Microsoft reports that in one year they alone purged over 13 million computers of Scareware. Such “digital extortion”, in different variants, is an increasing phenomenon to which both private individuals and companies can fall victim. Some examples:

- Compromised data that was “stolen” from the original owner is offered for repurchase.
- The attacker threatens to make public the successful attack on the data or IT infrastructure of a company. The company in question is told to pay “hush money”.

- The exaction of protection money, for example by threatening to carry out a DDoS attack on the company's IT infrastructure. Should the company refuse to pay, an attack is indeed carried out. But more on this later.

Ransomware works in a similar way. Ransomware infects, for example, the computer of victims while they are surfing the internet. A pop-up window appears claiming that the computer has been used for criminal acts and has therefore been locked. To unlock the computer the user has to pay a "fine" of €100 by means of a digital payment system. He is advised that the hard disk will be deleted if he fails to make the payment. Relatively small sums are demanded with a view to motivating as many infected victims as possible to make a payment. To create the impression that this is a police measure, the offenders use logos of police authorities and various well-known antivirus software vendors. In one particular case, over a period of only two days an offender in Germany attempted to infect 200,000 computers and was successful in 32,000 cases.

Numerous countries all over the world are meanwhile affected by this phenomenon. Adapted versions of Ransomware are now also circulated, for example, in North and South America. The reason for this is that the malware source code can be bought in the so-called underground economy (since late 2011).

2.5 Botnets

Cybercriminals often use so-called botnets to carry out their offences these are computers of usually unsuspecting victims which cybercriminals have infected with malware and gained control over. Once infected, the victim‘s computer is used to carry out attacks; it becomes an instrument of crime!

The dimensions botnets can take on can be seen from an example in Spain. A 23-year-old „bot herder“ had control over a global botnet („Mariposa“) with 12 million infected computers.

Early in June 2013, the United States carried out measures directed at the infrastructure of the so-called Citadel botnets.

Approximately 1,000 of an estimated total of 1,400 Command &Control Servers, servers to control bots, were deactivated in more than 80 countries. According to Microsoft, up to 5 million personal computers all over the world are thought to be infected by the Citadel malware.[7]

Following on from PC systems, cyber criminals are now increasingly focusing their attention on smartphones. These are infected by manipulated Apps. When a smartphone is infected it becomes part of a botnet and malware with other functions can be ins-

[7] Reuters, 06 June 2013

talled at any time. From the perpetrators' point of view the smartphone is the better bot! Modern smartphones are high-performance devices which are "always on" and permanently connected to the internet via modern high-speed networks.

It is examples like this which show that criminals analyse new technologies for potential illegal application, identify flaws and within a very short period develop methods to exploit these for their own purposes.

2.6 Underground Economy

A separate market has been established on the internet which provides everything cyber criminals require to carry out offences. The products available in the underground economy range from:

1. malware to
2. server capacity,
3. anonymous or encrypted communication channels,
4. services for creating false identities,
5. credit card data right up to
6. anonymous payment systems.

This illustrates how professionally organised and lucrative cybercrime is.

2.7 Attacks on Critical Infrastructures

For quite some time now the internet, and other services available on the internet, have themselves become critical infrastructures. As already mentioned, attacks can have fatal consequences for the economy and society. The borderlines between crime, espionage and terrorism are diffuse.[8]

A series of attacks directed at industrial facilities and critical infrastructures worldwide since 2010[9] has been a powerful reminder of the far-reaching consequences a cyber attack which exploits the flaws in a system can have.

Or: The consequences of a mass DDoS attack in March 2013 on the SPAMHAUS group, an organisation combating unwanted internet advertising, can be regarded as collateral damage. SPAMHAUS creates, among other things, real-time blacklists of spam senders in order to enable internet providers to filter out such authors. However, the attack not only blocked access to the SPAMHAUS website, but also resulted in a temporary breakdown of the UK's central internet node and slowed down large parts of the entire internet.

[8] FAZNET, 07 February 2011; DE MAIZIÈRE on the occasion of the Munich Security Conference

[9] The stuxnet trojan was first discovered in July 2010

2.8 Cyber bullying

However, let us not forget commonplace cases such as cyber bullying.

Cyber bullying is the use, mostly by pupils, of the internet or mobile phone to deliberately insult, threaten or harass over a long-term period. The perpetrators use the internet and mobile telephone services to humiliate and harass their victims. A whole range of internet services are used for this purpose such as emails, online communities, microblogs, chats, (chat rooms, instant messenger), discussion forums, guest books and boards, video and photograph platforms, web sites, and other applications. Mobile telephones are used for such bullying whereby calls, text messages, MMSs or emails are sent to the victim to tyrannize him or her. Today, mobile phones are equipped with cameras and video cameras, digital voice recorders and access to the internet, all of which facilitate bullying by means of easy-to-use technology.

The internet seems to lower the inhibition threshold for bullying activities. Many people seem to find it easier to attack, insult and humiliate someone in the apparently anonymous virtual world. The psychological face-to-face inhibition threshold no longer exists. There is a smooth transition from „fun“ to violence in terms of bullying. Statements such as, „I was only joking“ highlight the fact that such „practical jokers“ frequently have no sense of right and wrong and lack sufficient awareness of the consequences of their actions.

The fact that the internet never forgets, and by this I mean that even deleted contents can come to the surface again and again, means that the victim can be repeatedly confronted with the material even though the conflict with the perpetrator has been resolved. Cyber bullying can at times have tragic consequences. There are cases of pupils who committed suicide as a result of cyber bullying.

In 2011, 25,000 European children and teenagers between the ages of 9 and 16 were interviewed as part of the EU Kids Online study. They were asked about their experience with cyber bullying. Spread throughout Europe, 6% of the children and teenagers interviewed stated that over the last 12 months they had been the victim or perpetrator of cyber bullying. Five percent of children in Germany have had such experience with bullying, which means that Germany is slightly below the European average.

3. Suppression strategies

The threats posed by cybercrime are manifold. The Internet provides perpetrators with numerous opportunities to commit offences, innumerable potential victims and points of attacks. There is a significant potential for risks and extensive damage and, in our estimation, this is expected to increase over the coming years. Technical developments towards an „always on“ society will reinforce the effect. In this context the increasing popularity of smartphones and mobile computers such as tablets will play a decisive role.

3.1 Global Player Initiative

New forms of crime underline clearly that there is no alternative to a holistic suppression strategy.

Besides consistent operational action across agencies, it is essential to integrate the business sector in a network of information. In recent years the Bundeskriminalamt has increased its co-operation with the private sector. We have taken the initiative to start an intensive direct dialogue with the private sector, in particular with German global players who do business throughout the world. In the meantime, 58 companies have decided to enter into co-operation with our office.

Often, enterprises possess important information which can supplement intelligence held at our end and which can be incorporated in our early detection strategies. In return we can raise the business community‘s awareness of security risks. Businesses are then able to take the necessary protective measures.

3.2 IPPP

We believe that the expertise available in companies, research institutes, industry and science will have to be fully exploited in the fight against cybercrime to a much greater extent than has been the case so far. Moreover, we want to comply with the request made by numerous business enterprises and associations to establish a central point of contact for all questions related to cybercrime.

As a first step in the area of cybercrime, we entered into an institutionalised Public Private Partnership (iPPP) with the key actors of the banking sector.[10] This new co-operation platform with its “German Competence Centre for Cybercrime” (G4C), set up by major German banks, has an operational orientation. Cybercrime specialists from the BKA are attached to this centre. The aim here is to strengthen all aspects of efficient criminal prosecution in this area of crime.

3.3 Response recommendations in cases of cybercrime

The following applies to the private sector.

Anyone can be the victim of cybercrime. A study has shown[11] that small and medium-seized businesses are a favoured target for cyber criminals. 50 percent of all cyber attacks target companies with fewer than 2,500 staff, a third of the companies affected have fewer than 250 staff.

Such companies are easy prey for cyber criminals precisely because they think they are of no interest to cyber criminals and have therefore failed to establish adequate security

[10] Signing of co-operation agreement with G4C planned for 21 January 2014

[11] Symantec Corporation: Internet Security Threat Report 18/2013

precautions. At a first glance, the reasons given by the companies for not reporting attacks may seem plausible. Nevertheless, the consequences of such a policy are very counterproductive. As long as companies continue to conceal attacks they have identified, the authorities in charge will remain in the position that they will neither have an opportunity to carry out an investigation nor have an accurate overview of the true situation. The potential to cause damage increases if offences are not reported!

It is against this background that one should view the obligation to report cyber attacks, which policymakers are considering and which business circles reject

State police authorities and the BKA have drawn up “Response recommendations for the private sector in cases of cybercrime”. These guidelines are intended to provide targeted companies with concrete information on how they should respond to cyber attacks and remove any uncertainty they may have in connection with reporting such criminally relevant incidents. The interests of the law enforcement authorities and the companies are therefore given due consideration. The following are just some aspects:

- statutory basis is presented,
- recommendations for senior management and system administrators are provided,
- possibilities and principles of police investigative work are presented,
- and central contact points at the federal and state police are provided.

These recommendations are available in printed form or online at the BKA’s homepage www.bka.de.

But the principle applies that one can protect oneself from internet attacks.

1. PC protection: Computer protection using anti-virus programmes and a firewall should always be your first priority. As data carriers such as CDs and USB memory sticks are increasingly being used to spread malware, it is advisable to check these for viruses before use.
2. Emails and chat: Only open emails from senders you trust. Suspicious emails from people you do not know should be immediately deleted. Malware is often concealed in graphics or email attachments. Under no circumstances should you open suspicious data files!
3. Software: Be careful about which software or plug-ins you install. A healthy distrust helps: If you have any doubts regarding authenticity, then it is better to forgo the download or installation.
4. File sharing network: Anyone who shares files with people they do not know risks infecting his/her computer with malware programmes. Moreover, sharing music, films or software which is protected by copyright is a criminal offence and can, in addition to a fine and imprisonment, lead to a compensation claim on the part of the owners of the rights.

5. Online shopping: Numerous businesses are evaluated on shopping, auction and price-comparison sites. A positive evaluation can be an indication of professional business practices. In any case, a good portion of honest mistrust is advisable - especially with regard to web sites offering goods well below the market price.
6. Payment on the internet: One should be particularly careful when purchasing goods on the internet, especially where payment in advance is required. When making a payment, account and credit card details should be transmitted via an encrypted connection.
7. Online banking: The connection to the computer used for banking purposes must, as is the case when making online payments, be encrypted. There are frequent new protection processes such as iTAN, eTAN and HBCI. You should contact your bank and select the latest process.
8. Private information and passwords: Do not use the same password for multiple services - for example email accounts, online shops and communities. The longer a password is, the more difficult it is to crack.
9. Offers to become a goods or financial agent: Any offers received on the internet or by email to work as a goods or money agent should be strictly rejected. If you comply with dubious offers and forward goods or money, you are aiding and abetting fraud or money laundering and will have to face criminal proceedings and claims for compensation.
10. Apps and subscription tricks: You should be aware of the fact that apps involve costs and can transmit sensitive data. You should be wary of any apps which are free of charge. Caution is called for with online services which require registration. Amongst the mass of serious promotion offers there are cases where people are unconsciously duped into ordering goods or entering into subscription contracts.

I therefore appeal to you: The responsible use of the internet lies in your hands!

4. Conclusion

The internet has become an indispensible pillar of global economic, political and social information and communication processes, but also provides the breeding ground for all sorts of criminal activity.

We must not allow the internet to become an area where the law does not apply. Crime suppression must be possible here too in order to bolster confidence in the internet and maintain its advantages.

In order to be able to successfully counter internationally active and networked cybercrime, a culture of trusting co-operation between the security authorities is required. We are facing joint challenges which we have to tackle in a concerted and coordinated way and on which we need to share our knowledge.

Companies, and ultimately also the general public, must raise their awareness of the situation and take responsibility for their own actions. I therefore welcome this special event on cybersecurity within the framework of the German Congress on Crime Prevention.

Content

Lectures and Documents from the 8th Annual International Forum