Expert Report: Aspects of Cyber Identify Theft in Germany

Word count: 2711

Principles of Digital Forensics and Cyber Law

MSc Cyber Security

July 2022

Cyber Identity Theft in Germany

The most common cyber identify thefts in Germany are when a cybercriminal obtains your identity to order software, to pay for online streaming services, to purchase a mobile phone in your name or to shop in general at an E-commerce store. All this is of course happening on the expense of the person which fell victim to the identity theft. Cyber identity theft in Germany can be conducted when you have either stolen credit card information or access to an already existing online shop account, where the cybercriminal can easily reroute the packages s/he is ordering with the intent to steal them from the victim. (Verbraucherzentrale, 2021)

The financial impact of victims of identity theft varies a lot. It can start from silently using you streaming account in parallel, where you almost have no financial impact to e.g., ordering expensive consumer goods, where the financial damage to an individual can be significant. Extreme cases are known in Germany with damages up to 50.000 EUR. The nationwide sum of damages caused by identity theft is however lower than the damages from ransomware attacks in Germany, nonetheless identity theft is also a pressing issue, since stealing the data and abusing the personal information can be done from places, where German authorities cannot effectively prosecute. Additionally it also needs to be stated that the damages in identity theft are rising every year significantly, similar like the damages in cybercrimes in general are increasing year by year. (Bundeskriminalamt, 2021b; Verbraucherzentrale, 2021; Bundeskriminalamt, 2022)

Legislation and Ethics in relation to Cyber Identify Theft

Germany transferred the directive of the European commission 95/46/EC into national law and additionally also published the Bundesdatenschutzgesetz (BDSG), where nationwide laws were brought into power, that dealt with the processing of employee data, video surveillance, data safety officers, etc. to close gaps in the directive 95/46/EC. In 2016 the EU parliament published the GDPR also known as EU regulation 2016/679. At the exact same time Germany published a revised version of their Bundesdatenschutzgesetz (BDSG). The BDSG is in case of any conflict overruled by the GDPR, since the European law is the primary law to use in Germany. National amendments like the BDSG are used secondary. Since EU regulations do not need to be amended by the member states, the GDPR is law that is fully applicable in Germany without any alteration or transferal. GDPR and BDSG therefore are the base for legislation on data protection in Germany. Those two laws are however not the only laws that are necessary when it comes to dealing with cybercriminals that conduct identity theft. Another law worth mentioning is the German penal code called Strafgesetzbuch StGB. The StGB has many paragraphs that support the conviction of cyber criminals. One of the paragraphs for example is §276 Urkundenfälschung. This paragraph outlines that the forging of documents is illegal and that a criminal may be imprisoned depending on the severity of the crime committed. (European Parliament and Council, 1995, 2016; Bundesministerium der Justiz, 2017; Müller, 2017; Bundesministerium der Jusitz, 2021)

The GDPR list many forms of personal data that need protection. It lists direct personal data like name, address, etc. for example. It however also lists indirect personal data where the identity is not directly revealed, but may be revealed with investigation, guess work or large datasets for example. An example of indirect data is location data as well as an identifier used in a database. The GDPR also lists types of data that need special protection like health records or biometric data. Both data types are valuable assets cyber criminals want to steal, since it is for example very easy with a comprehensive health data set to pretend to be a person and to conduct subsequent identity theft. Biometric data like fingerprints can be used by a cybercriminal for example to open a stolen mobile phone and then to e.g., authorize money transfers via online banking. The GDPR has many paragraphs that can be used to convict cyber criminals. One of them being that private data must be processes lawfully and fairly for example. On the other hand, the GDPR also provides requirements for entities storing and processing the data. A requirement for example is that private data must be protected and always safeguarded from unauthorized access. This law not only likely improves cyber security and therefore makes it harder to hack a company and to prevent identity theft in the first place, it also gives victims another possibility to get compensation for any harm they had to endure due to inadequate security of their private data. (European Parliament and Council, 2016)

Even though it is undoubtably ethically incorrect to conduct cyber identity theft, since person are severely harmed in some cases, the fact still persists that identity theft is conducted with increasing frequency in Germany. This raises the question if the law in Germany is effective or not or if other factors might hinder the prosecution of criminals that obviously act unethically (Bundeskriminalamt, 2021b; Verbraucherzentrale, 2021; Bundeskriminalamt, 2022)

Effect and limitation of law applicable in Germany on Cyber Identify Theft

Since the GDPR has implications for companies such as the requirement that they must safeguard personal data acquired for example and since the GDPR is also enforced by local courts with high fines, it can be stated that it is very likely that there is an effect that personal data is better safeguarded in the future or is already safeguarded better now. This is likely due to the fact that penalties of the GDPR are severe, and this seems to be an effective incentive for companies to invest in cyber security to prevent paying for hefty legal penalties. (European Parliament and Council, 2016; Bodoni, 2022; Collins, 2022; Pfann, 2022)

One issue that hinders an effective combat of cyber crime and cyber identity theft however is the fact, that many people do not go to law enforcement agencies to report their crime. Another issue affecting the effective combat of cybercrime in Germany is that most law enforcement agencies currently are not trained to handle cybercrime. In some cases, it was even reported that the police in Germany is not aware that it is their duty to act when someone files charges in relation with cybercrime. It was even reported that the police send people away that had legit reasons to file charges. (Deckner, 2022; Maier, 2022; Mewes, 2022)

Another limitation of the GDPR, the StGB and of the BDSG to come fully into effect is the fact that the GDPR can only be utilized in Europe and that StGB and BDSG can only be utilized in Germany, whilst many crimes are committed from outside of Germany and Europe. Germany as well as Europe is member of many multilateral and bilateral treaties like the UN Convention against Transnational Organized Crime UNTOC or member of the EUROPOL's Joint Cybercrime Action Taskforce (J-CAT) for example. This effective network of agreements supports the prosecution of many cyber criminals outside of Germany and even outside of the European union. It needs to however be stated that such contracts do not exist with every government on the world. Moreover, it must be said, that some countries seem to effectively safeguard their cybercriminals conducting offenses. These state sponsored hacking groups primarily conduct ransomware attacks, but also might be an integral element of obtaining personal data, that is sold and then later used by other criminals that conduct subsequent identity theft. The fact that legislation cannot effectively be fully enrolled globally is the major contributor that cyber crime remains high. (Peters and Hindocha, 2016; Ajoy, 2022; Kari, 2022; Lyngass, 2022; Milmo and Kari, 2022; Nayyar, 2022; Wilkie, 2022)

Effect and limitation of investigative tools available in Germany in dealing with Cyber Identify Theft

Tools such as Encase, FTK, X-Ways Forensics offer various features that can be helpful with the challenges of investigation cyber identity theft. They however also do have their limitations with is described in the following.

One of the biggest challenges for cyber forensics experts is that professional cyber criminals maintain the anonymity since they skillfully use tools like the onion router also called TOR and proxy servers to hide their identity by leaving traces of IP addresses that cannot be connected to the real-world addresses. Not so skilled criminals on the other hand can be identified by leaving an IP address, that can be connected to their real-world location in communication logs for example. Forensic tools are ideal tools to scan a victim’s computer for IP address in the various logs of the many services a modern operating system offers. In cases where the cybercriminal is not skilled the forensic tools can have great effect. In cases where the cybercriminal however is very skilled the limitation of the tool is immediately visible. It still outputs an IP address. This IP address is however not connectable to a real-world location which is essential to arrest the cybercriminal. (Jaishankar, 2011; Holt, Bossler and Seigfried-Spellar, 2015; Amoroso, 2021)

In case a cybercriminal is skilled it is necessary to attribute the crime to the criminal. Common ways to attribute a crime to a certain group is to monitor when they are active, which provides conclusions in which time zone they reside. Another way of attributing a crime to a group is by identifying the methods and tools that were used. A group has its very own fingerprint on what tools they use and how they are being used. REvil for example uses malware and tools like cerbutil, cobalt strike, etc. whereas Cozy Bear uses tools like WellMess and Ceeloader. The tools leave very unique traces while being used, which helps to attribute a cyber crime to an organization, which supports in some case further investigation by e.g. obtaining a surveillance warrant for individuals, if they are in the jurisdiction. Modern forensic tools might be able to support with this type of activity by looking for traces of those tools e.g. by signature based scanning. (Jaishankar, 2011; Holt, Bossler and Seigfried-Spellar, 2015; Amoroso, 2021; Morgan, 2021; Bundeskriminalamt, 2022)

To have evidence that is admissible in court the forensic evidence must be collected according to the requirements of the court of that country. Different countries do have different requirements on how evidence shall be obtained, preserved, and shared. This is a tremendous challenge for the digital forensic expert. The lack of harmonization of evidence collection is also a factor that contributes to the fact that collecting digital evidence manually is a hard task, since the different national requirements must be known to the forensic expert. Automated tools do have workflows, methods and techniques that support with this kind of activity. Since the admission of evidence is a case-by-case decision it is obvious that even tools cannot foresee all eventualities that are to be followed when collecting certain digital evidence. It is likely that even if with the usage of tools that some evidence is not admissible in court. The tools are nonetheless likely to be superior in the collection of evidence compared to a manual collection. (Jaishankar, 2011; Holt, Bossler and Seigfried-Spellar, 2015; Caviglione, Wendzel and Mazurczyk, 2017; Amoroso, 2021)

Challenges for the future in obtaining forensic evidence is the fact that the amount of data is increasing by the day. The readout out of network logs of bigger servers might be too time consuming in the future. Methods like reading out areas of interest only, like reading out the firewall log or a honeypot log seem to be something that needs to be considered. It is also hard or even not feasible to scan data that is encrypted which is more and more common on many devices nowadays. Another trend seen in cyberattacks is that criminals use methods and tools to hinder the investigation by automatically wiping logs or leaving false traces. In summary it can be stated, that digital forensics is continuously challenged by the rapid evolvement of technology itself and must evolve with a similar pace to not be left behind. (Jaishankar, 2011; Holt, Bossler and Seigfried-Spellar, 2015; Caviglione, Wendzel and Mazurczyk, 2017)

Evaluation of aspects concerning victims, harm, cyber criminals, and social perception

Victimization happens when there is a motivated offender, a suitable victim, and an absence of a guardian. In the case of identity theft there is a plethora of offenders due to lack of gapless international prosecution. Suitable targets are also available since credit cards generally offer a relatively high credit limit in general for example. The last item, the lack of guardian is however the element where an individual can change the fact whether s/he becomes a victim. In the cybercrime space a guardian can simply be a suitable tool or program. Antivirus software for example is an effective tool, that makes it harder for cybercriminals to steal credentials and credit card information in the first place. By choosing a good bank, that offers settings for credit cards one can also increase the personal protection. Some banks offer for example the feature that credit cards can only be used in countries that are chosen by the owner of the card. (Jaishankar, 2011; Holt, Bossler and Seigfried-Spellar, 2015; Buchanan, 2019)

It was identified that harm from cybercrime that is conducted online can manifest in the real world. There are examples of cyber bullying where the victim committed suicide. With cyber identity theft the harm might not be as dramatic in most cases as with cyber bullying, however the loss of 50.000 EUR in extreme cases of identity theft is definitely a severe challenge for one’s life. (Jaishankar, 2011; Holt, Bossler and Seigfried-Spellar, 2015; Randa and Reyns, 2019; Bundeskriminalamt, 2021b; Verbraucherzentrale, 2021; Bundeskriminalamt, 2022)

The effects on cybercriminals vary a lot. Those how are knowledgeable can conduct their offenses with no punishment at all in most cases. The ones with less skills that cannot masquerade their IP properly for example can expect some jailtime. There is however a very small number of cases where the most skilled cyber criminals are prosecuted by authorities with highest efforts. An example is the recent conviction of a member of the group REvil in the Bahamas, where German authorities spent a lot of resources and waited till the cybercriminal travelled to a country where Germany had an agreement for extradition. (Jaishankar, 2011; Biermann, 2014, 2021; Prantl, 2021)

The social perception of most people is that cybercrime including identity theft is a growing issue. People are also aware that they must act carefully in cyberspace in general. It needs to however also be said, that people know that some cybercriminals cannot be prosecuted, which leads to the fact that some people do not go to the police to file charges (Deckner, 2022; Maier, 2022; Mewes, 2022)

Conclusion

In conclusion it can be said that identity theft is a growing issue. Whilst the legislation has improved with the GDPR significantly, it is still a concern that such a law cannot be applied globally. On the contrary it is even the case that some government actively protect criminals, which is a major problem for cyber identity theft since it is a transnational crime.

Tools in cyber forensics play a key role, since there are many challenges like huge data volumes, various location for essential log files, different requirements in how to collect evidence that is admissible in the respective country, etc. where tools make a significant difference compared to manual work.

Victims of identity theft may in extreme cases perceive a very high level of harm, so it should not be taken lightly. It can however also be said that there are methods and tools available, that reduce the likeliness to become a victim significantly or at least to limit the damage. Whilst most cyber criminals remain unprosecuted, there is a small number of cases where they do get very high jail times.

(Bryant and Bryant, 2006; Jewkes and Yar, 2013; Warwick, 2014; European Parliament and Council, 2016; Marques-Arpa and Serra-Ruiz, 2016; Umhoefer, 2018; Buchanan, 2019; Randa and Reyns, 2019; Verbraucherzentrale, 2021; Bundeskriminalamt, 2021a, 2022; Bundesministerium der Jusitz, 2021)

References

Ajoy, P. (2022) ‘Effectiveness of Criminal Law in Tackling Cybercrime: A Critical Analysis’, *Scholars International Journal of Law, Crime and Justice*, 5(2), pp. 74–79. doi: 10.36348/sijlcj.2022.v05i02.005.

Amoroso, E. G. (2021) *Your Guide to OpenText and Filogix Collaborative Document Solutions Modernizing Enterprise Forensic Investigation*. Available at: https://www.opentext.com/info/security/digital-forensics/.

Biermann, K. (2014) *Computerkriminalität: Das Gesetz, das keine guten Hacker kennt | ZEIT ONLINE*. Available at: https://www.zeit.de/digital/internet/2013-03/hacker-weev-auernheimer (Accessed: 15 July 2022).

Biermann, K. (2021) *Ransomware-Group REvil: Core member of ransomware gang identified | ZEIT ONLINE*. Available at: https://www.zeit.de/digital/internet/2021-10/ransomware-group-revil-member-hacker-russia-investigation (Accessed: 15 July 2022).

Bodoni, S. (2022) *Amazon (AMZN) Given Record $888 Million EU Fine for Data Privacy Breach - Bloomberg*. Available at: https://www.bloomberg.com/news/articles/2021-07-30/amazon-given-record-888-million-eu-fine-for-data-privacy-breach (Accessed: 14 July 2022).

Bryant, R. and Bryant, S. (2006) *Policing Digital Crime*. Available at: https://ebookcentral.proquest.com/lib/universityofessex-ebooks/reader.action?docID=4511974.

Buchanan, R. (2019) ‘What We Know about Identity Theft and Fraud Victims from Research-and Practice-Based Evidence CENTER for VICTIM RESEARCH Research Report’, (August), p. 34. Available at: https://ncvc.dspacedirect.org/bitstream/handle/20.500.11990/1544/CVR Research Syntheses_Identity Theft and Fraud_Report.pdf?sequence=1&isAllowed=y.

Bundeskriminalamt (2021a) *Cybercrime*. Available at: https://www.bka.de/DE/UnsereAufgaben/Deliktsbereiche/Cybercrime/cybercrime_node.html (Accessed: 14 July 2022).

Bundeskriminalamt (2021b) *Identitätsdiebstahl/Phishing*. Available at: https://www.bka.de/DE/IhreSicherheit/RichtigesVerhalten/StraftatenImInternet/Identitaetsdiebstahl/identitaetsdiebstahl_node.html (Accessed: 14 July 2022).

Bundeskriminalamt (2022) ‘National Situation Report on Cybercrime 2021’. Available at:

https://www.bka.de/SharedDocs/Downloads/DE/Publikationen/JahresberichteUndLagebilder/Cybercrime/cybercrimeBundeslagebild2021.html;jsessionid=B23C0470BCF1301BDC4EE6E0072A164D.live291?nn=28110.

Bundesministerium der Jusitz (2021) *Strafgesetzbuch StGB*. Available at: https://www.gesetze-im-internet.de/stgb/ (Accessed: 14 July 2022).

Bundesministerium der Justiz (2017) *Bundesdatenschutzgesetz*. Available at: https://www.gesetze-im-internet.de/bdsg_2018/ (Accessed: 14 July 2022).

Caviglione, L., Wendzel, S. and Mazurczyk, W. (2017) 'The Future of Digital Forensics: Challenges and the Road Ahead', *IEEE Security and Privacy*, 15(6), pp. 12–17. doi: 10.1109/MSP.2017.4251117.

Collins, K. (2022) *GDPR Fines: The Biggest Privacy Sanctions Handed Out So Far - CNET*. Available at: https://www.cnet.com/tech/gdpr-fines-the-biggest-privacy-sanctions-handed-out-so-far/ (Accessed: 14 July 2022).

Deckner, S. (2022) *'ZDF Magazin Royale': Böhmermanns entlarvendes Experiment belastet die Polizei*. Available at: https://www.stern.de/kultur/tv/-zdf-magazin-royale---boehmermanns-entlarvendes-experiment-belastet-die-polizei-31901710.html (Accessed: 14 July 2022).

European Parliament and Council (1995) *95/46/EC Data Protection Directive*.

European Parliament and Council (2016) *2016/679/EU General Data Protection Regulation GDPR*.

Holt, T., Bossler, A. and Seigfried-Spellar, K. (2015) *Cybercrime and Digital Forensics*, *Cybercrime and Digital Forensics*. Taylor and Francis. doi: 10.4324/9781315777870.

Jaishankar, K. (2011) *Cyber Criminology*, *Cyber Criminology*.

Jewkes, Y. and Yar, M. (2013) *Handbook of Internet Crime*.

Kari, P. (2022) *'Lives are at stake': hacking of US hospitals highlights deadly risk of ransomware*. Available at: https://www.theguardian.com/technology/2022/jul/14/ransomware-attacks-cybersecurity-targeting-us-hospitals (Accessed: 14 July 2022).

Lyngass, S. (2022) *North Korean government hackers hit health services with ransomware, US agencies warn*. Available at: https://edition.cnn.com/2022/07/06/politics/north-korea-ransomware-health-care/index.html (Accessed: 14 July 2022).

Maier, U. (2022) *Nach Böhmermann-Sendung: Bessere Bekämpfung von Hass im Netz gefordert*. Available at: https://www.tagesschau.de/inland/polizei-hassverbrechen-internet-101.html (Accessed: 14 July 2022).

Marques-Arpa, T. and Serra-Ruiz, J. (2016) ‘Procedure for Obtaining and Sharing the Digital Evidence’, *International Journal of Chaotic Computing*, 4(1), pp. 79–86. doi: 10.20533/ijcc.2046.3359.2016.0010.

Mewes, B. (2022) *Böhmermann: Recherche zur Anzeige von Hasskommentaren löst Reaktionen aus | heise online*. Available at: https://www.heise.de/news/Boehmermann-Recherche-zur-Anzeige-von-Hasskommentaren-loest-Reaktionen-aus-7125394.html (Accessed: 14 July 2022).

Milmo, D. and Kari, P. (2022) *Russia-backed hackers behind powerful new malware, UK and US say*. Available at: https://www.theguardian.com/world/2022/feb/23/russia-hacking-malware-cyberattack-virus-ukraine (Accessed: 14 July 2022).

Morgan, C. (2021) *Cyber Attacks: The Challenge of Attribution and Response*. Available at: https://www.digitalshadows.com/blog-and-research/cyber-attacks-the-challenge-of-attribution-and-response/ (Accessed: 14 July 2022).

Müller, N. (2017) *Die Bedeutung der Datenschutz-Grundverordnung für das Ar ... / 1.2 Verhältnis zwischen BDSG und DSGVO*. Available at: https://www.haufe.de/personal/haufe-personal-office-platin/die-bedeutung-der-datenschutz-grundverordnung-fuer-das-ar-12-verhaeltnis-zwischen-bdsg-und-dsgvo_idesk_PI42323_HI11404989.html (Accessed: 14 July 2022).

Nayyar, S. (2022) *How To Protect Your Intellectual Property From State-Sponsored Hackers And Insiders*. Available at: https://www.forbes.com/sites/forbestechcouncil/2022/06/15/how-to-protect-your-intellectual-property-from-state-sponsored-hackers-and-insiders/?sh=35f902406380 (Accessed: 14 July 2022).

Peters, A. and Hindocha, A. (2016) *US Global Cybercrime Cooperation: A Brief Explainer*. Available at: https://www.thirdway.org/memo/us-global-cybercrime-cooperation-a-brief-explainer (Accessed: 14 July 2022).

Pfann, A. (2022) *Datenschutz: Google und Facebook müssen Millionenstrafe in Frankreich zahlen*. Available at: https://www.zeit.de/wirtschaft/2022-01/datenschutz-frankreich-google-facebook-millionenstrafe-cookies?utm_referrer=https%3A%2F%2Fwww.google.com%2F (Accessed: 14 July 2022).

Prantl, H. (2021) *Hacken, ausspähen, abfangen - was alles strafbar ist - Digital*. Available at: https://www.sueddeutsche.de/digital/hackerangriff-strafrecht-1.4277701 (Accessed: 15 July 2022).

Randa, R. and Reyns, B. W. (2019) 'The Physical and Emotional Toll of Identity Theft Victimization: A Situational and Demographic Analysis of the National Crime Victimization Survey', *https://doi.org/10.1080/01639625.2019.1612980*, 41(10), pp. 1290–1304. doi: 10.1080/01639625.2019.1612980.

Umhoefer, C. (2018) *Die Auswirkungen der DSGVO auf interne Untersuchungen | | Insights | DLA Piper Global Law Firm*. Available at: https://www.dlapiper.com/de/germany/insights/publications/2018/07/global-anticorruption-newsletter/the-gdpr-impact-investigations/ (Accessed: 28 June 2022).

Verbraucherzentrale (2021) *Welche Folgen Identitätsdiebstahl im Internet haben kann*. Available at: https://www.verbraucherzentrale.de/wissen/digitale-welt/datenschutz/welche-folgen-identitaetsdiebstahl-im-internet-haben-kann-17750 (Accessed: 14 July 2022).

Warwick, A. (2014) *Annual global cost of identity theft as high as £3bn*. Available at: https://www.computerweekly.com/news/2240214217/Annual-global-cost-of-identity-theft-as-high-as-3bn (Accessed: 4 July 2022).

Wilkie, C. (2022) *U.S., NATO and EU to blame China for cyberattack on Microsoft Exchange servers*. Available at: https://www.cnbc.com/2021/07/19/nato-and-eu-launch-a-cyber-security-alliance-to-confront-chinese-cyberattacks.html (Accessed: 14 July 2022).