УДК 343:004

DIE SPRACHE DER CYBERKRIMINALITÄT

Čapek Jan
PhDr, Profesor, Katedra cizích jazyků, Fakulta filozofická,
Univerzita Pardubice (Pardubice, Česko)
e-mail: jan.capek@upce.cz

Im Artikel geht es um den Begriff Cyberkriminalität (Internetkriminalität, Cybercrime bzw. Internet- und Computerkriminalität/IuK-Kriminalität), der sich auf Straftaten bezieht, die mit oder gegen moderne Informations- und Kommunikationstechnik begangen werden. Der Autor berücksichtigt die Arten der Cyberkriminalität.

Schlüsselworte: der Begriff, die Cyberkriminalität, die Straftat, die Daten, der Diebstahl, der Nutzer, die Gefahr

The article is about the term cybercrime. It refers to crimes committed with or against modern information and communication technologies. The author considers the types of cybercrime.

Keywords: term, cybercrime, crime, data, robbery, user, danger

1. Einführung und Definition

Unter dem Begriff Cyberkriminalität (Internetkriminalität, Cybercrime bzw. Internet- und Computerkriminalität/IuK-Kriminalität) versteht man Straftaten, die unter Ausnutzung moderner Informations- und Kommunikationstechnik oder gegen diese begangen werden. Es sind folgende Straftaten:

– alle Straftaten, bei denen Elemente der EDV in den Tatbestandsmerkmalen enthalten sind (Computerkriminalität) oder bei denen IuK zur Planung, Vorbereitung oder Ausführung einer Tat eingesetzt wird,

– Straftaten im Zusammenhang mit Datennetzen wie z.B. dem Internet,

– Fälle der Bedrohung von Informationstechnik – dies schließt alle widerrechtlichen Handlungen gegen die Integrität, Verfügbarkeit und Authentizität von elektronisch gespeicherten oder übermittelten Daten (Hacking, Computersabotage, Datenveränderung, Missbrauch von Telekommunikationsmitteln etc.) ein.

2. Liste von einzelnen möglichen Straftaten

Die Definition ist sehr weit gefasst und drückt die Vielfalt von aktuellen Kriminaltaten aus, die im, mit dem, durch das und auf das Medium Internet Bezug nimmt und mit der dynamischen Entwicklung der EDV-Technik zusammenhängt.

Bei Computerkriminalität im engeren Sinne handelt es sich um Delikte wie Computerbetrug, das Ausspähen und Abfangen von Daten, die Datenveränderung

sowie die Datensabotage, Fälschung beweiserheblicher Daten oder die Störung öffentlicher Betriebe. Unter Computerkriminalität im weiteren Sinne zählen Straftaten, zu deren Durchführung einer ihrer Phasen ein elektronisches Datenverarbeitungssystem unter Einbezug von Informations- und Kommunikationstechnik genutzt wird. Dazu werden der Warenkreditbetrug, Propagandastraftaten aus extremistischen Kreisen, Gewaltverherrlichung, das Verbreiten von Kinderpornographie oder Beleidigungstatbestände gerechnet. Mit der weltweiten Zunahme der Internetnutzung wird die Verbreitung strafbarer Inhalte dieser Kategorie vereinfacht.

Aus der Definition lassen sich folgende Tathandlungen ableiten: Missbrauch der vorhandenen gespeicherten Daten (Phishing, Betrug, Urheberrechtsverletzungen, Kreditkartenmissbrauch oder Propagandastraftaten, Cybermobbing), neue Daten werden generiert und veröffentlicht (Verbreitung von Kinderpornographie, terroristischer Ideologien, Gewaltdarstellungen, Aufstachelung zum Rassenhass, Angriffe auf das Medium Internet (Verbreitung von Viren, Würmer und Trojaner, Eindringen in PC-Anlagen zur Datenänderung, Datenlöschung oder zum Datendiebstahl führende Attacken.

3. Kurze Beschreibung von einzelnen Arten

3.1. Identitätsdiebstahl

Der Identitätsdiebstahl ist das Aneignen digitaler persönlicher Merkmale einer Person (Benutzername und Passwort einer natürlichen oder juristischen Person in einer Bank, in einem Webshop zum Internetbanking, Einkaufen/Verkaufen bis zum Aufbau einer Parallelwelt), missbräuchliche Nutzung personenbezogener Daten durch Dritte – Identitätsmissbrauch oder gar die Einrichtung von Fake-Accounts für Beleidigungen, sexuelle Anspielungen oder Unwahrheiten über dritte Personen, Länder, politische Parteien usw.

3.2. Social engineering, social hacking

Angriff auf das Firmennetzwerk, neben dem klassischen „Hacken“ von Computern ist es Diebstahl von Informationen und Daten. Versand persönlicher Emails mit der Aufforderung, aus bestimmten Gründen vertrauliche Informationen preiszugeben (Verifizierung des Online-Banking-Accounts), Enkel-Neffen-Trick (Human-based-social-engineering): Nach dem Namen eine ältere Person aus dem Telefonbuch ausgewählt, der Anrufer gibt sich als Enkel der angerufenen Person aus, befindet sich in einer finanziellen Not und braucht dringend schnell Bargeld. Verschiedene Vorwände, warum man dann das Geld nicht persönlich übernehmen kann (Krankheit).

3.3. Phishing

Phishing ist das unbefugte Beschaffen und Nutzen von Zugangsdaten fremder Personen (Passwörter, PIN), also das „Abfischen“ von persönlichen Daten (ein Neologismus von *password* und *fishing*, also „Passwortangeln“.

Beispiel für den Inhalt einer Phishingmail:

Sehr geehrter Kunde, die Sparkasse arbeitet derzeit an technischen Arbeiten in der Abteilung Internetbanking. Dieser Abschnitt befasst sich mit der Installation einer neuen Software zur Sicherung Ihres Internetbanking-Kontos. Mit diesem Service wird die Bank Ihr Konto vor Spam, Cyberkriminalität und unberechtigtem Zugriff auf Ihr Konto durch Dritte schützen.

Um diesen Service zu nutzen, empfehlen wir Ihnen den Link unten anzuklicken und die erforderlichen Informationen für die Aktualisierung einzureichen.

Nach Abschluss der Vervollständigung Ihrer Daten wird Ihr Internetbanking-Konto automatisch aktualisiert. Wir bedanken uns für Ihr Vertrauen und verbleiben mit freundlichen Grüßen. Sparkasse Kundendienst.

3.4. Internetbanking, Onlinebanking

Missbrauch von Bankgeschäften (Überweisungen, Banksoftware, Clientprogramm, Hackerprogramme zum „Erraten" von PIN, durch Malware wird dem Kunden am PC vorgespielt, er müsse seine Zugangsdaten synchronisieren…).

3.5. Skimming

Das elektronische Auslesen des Magnetstreifens einer Bank- oder Kreditkarte – *to skim – abschöpfen, absahnen*), wobei der Geldautomat manipuliert wird oder ein Kartenleser am Türöffner des Geldinstituts installiert wird.

3.6. Ransomware (Online-Erpressungen)

Eine solche Schadsoftware, die den Nutzer erschrecken soll bzw. ihm Angst einjagen soll, um ihn am PC Handlungen ausführen zu lassen, die er sonst nicht tätigen würde. Der Name setzt sich aus dem englischen Wort *ransom* für Erpressung und *ware* für Schadsoftware zusammen. Dem Betroffenen wird suggeriert, dass sein Computer mit Viren befallen wird, dagegen wird günstige Software zum Download angeboten oder werden vermeintliche Antivirenschutzprogramme angeboten, die nach der Installation persönliche Daten verschlüsseln und erst nach der Zahlung eines „Lösegeldes" werden sie wieder entschlüsselt. Eine andere Möglichkeit ist „Trojaner", der den infizierten Rechner sperrt, sodass an diesem kein Arbeiten mehr möglich ist. Nur gegen eine vorgebliche „Strafzahlung" via elektronischem Zahlungsmittel soll dieser wieder frei geschaltet werden. Beispiel einer Erpressung:

Hohe Gefahr. Konto wurde angegriffen

Hallo!

Wie Sie vielleicht bemerkt haben, habe ich ***Ihnen*** *eine E-Mail von Ihrem Konto aus gesendet. Dies bedeutet, dass ich vollen Zugriff auf* ***Ihr*** *Konto habe. Ich habe* ***dich*** *jetzt seit ein paar Monaten beobachtet. Tatsache ist, dass* ***Sie*** *über eine von* ***Ihnen*** *besuchte Website für Erwachsene mit Malware infiziert wurden.*

*Wenn **Sie** damit nicht vertraut sind, erkläre ich es **Ihnen**. Der Trojaner-Virus ermöglicht mir den vollständigen Zugriff und die Kontrolle über einen Computer oder ein anderes Gerät. Das heißt, ich kann alles auf **Ihrem** Bildschirm sehen, Kamera und Mikrofon einschalten, aber **Sie** wissen nichts davon. Ich habe auch Zugriff auf alle **Ihre** Kontakte und **Ihre** Korrespondenz (...) Mit einem Mausklick kann ich dieses Video an alle **Ihre** E-Mails und Kontakte in sozialen Netzwerken senden. Ich kann auch Zugriff auf alle **Ihre** E-Mail-Korrespondenz und Messenger, die **Sie** verwenden, posten. Wenn **Sie** dies verhindern möchten, übertragen Sie den Betrag von 390€ an meine Bitcoin-Adresse (wenn Sie nicht wissen, wie Sie dies tun sollen, schreiben Sie an Google: „Buy Bitcoin"). Meine Bitcoin-Adresse (BTC Wallet) lautet: 1G1qFoadiDxa7zTvppSMJhJi63tNUL3cy7 Nach Zahlungs-eingang lösche ich das Video und **Sie werden mich nie wieder hören**. Ich gebe **dir** 48 Stunden, um zu bezahlen. Ich erhalte eine Benachrichtigung, dass **Sie** diesen Brief gelesen haben, und der Timer funktioniert, wenn **Sie** diesen Brief sehen. Eine Beschwerde irgendwo einzureichen ist nicht sinnvoll, da diese E-Mail nicht wie meine Bitcoin-Adresse verfolgt werden kann. Ich mache keine Fehler. Wenn ich es herausfinde, dass **Sie** diese Nachricht mit einer anderen Person geteilt haben, wird das Video sofort verteilt. Schöne Grüße!*

3.7. Hacken von Telefonanlagen

In die Verbindung zwischen Deutschland und Ausland mischen sich betrügerische Provider.

3.8. Finanzagent, Warenagent

Es werden Werbemails mit angebotenen Nebenjobs oder hauptamtlichen Berufsausübung versendet, wo ein Konto für Transferzahlungen zur Verfügung gestellt wird (Finanzagent). Alternativ werden die Bewerber dazu missbraucht, Waren in Empfang zu nehmen, die mit ausspionierten Konto- oder Kreditkartendaten auf Kosten der Opfer bezahlt wurden (Warenagent).

3.9. Urheberrecht

Die Regelungen des Urheberrechts gelten auch bei der Nutzung des Internets, sowohl beim Bezug des Angebots, als auch bei der Gestaltung von Inhalten, die im Netz veröffentlicht werden. Es wird dabei das geistige Eigentum und Verwertungsrecht geschützt. Den Schutz des Urheberrechtes genießen Sprachwerke, Schriftwerke, Reden und Computerprogramme, Werke der Musik, der bildenden Künste einschließlich der Werke der Baukunst und angewandten Kunst, Filmwerke, Darstellungen wissenschaftlicher oder technischer Art, Zeichnungen, Pläne, Karten, Skizzen, Tabellen. Verstöße gegen das Urheberrechtgesetz können das Herunterladen, Tauschen von Musik- und Filmdateien sowie das Kopieren von Texten und Bildern aus dem Netz sein – auch wenn es zu nichtkommerziellen Zwecken geschieht.

3.10. Kinderpornographie

Darstellung sexueller Handlungen von, an und vor Kindern. Es handelt sich um die Darbietung dieser Handlungen auf Ton- und Bildträgern, Datenspeichern, Abbildungen und anderen Darstellungen (z.B. Comics).

3.11. Cybermobbing

Jemand ist Gewalt ausgesetzt oder wird gemobbt, wenn er/sie wiederholt und über eine längere Zeit den negativen Handlungen einer oder mehrerer Personen ausgesetzt ist (psychische Gewalttätigkeiten, Beleidigungen, üble Nachreden, die Bloßstellung oder das Ausschließen aus der Gruppe – alles unter der Benutzung von World Wide Web. Hasserfüllte Foren, persönliche Attacken. *Mobbing* entstammt aus dem Englischen – *anpöbeln (to mob)* oder *Pöbel (mob),* daher Internetmobbing.

Beispiel: Forum 4chan und Angriffe auf Jan Böhmermann, der das Internet vor rechten Trollen retten wollte (durch die Aktion „Reconquista Internet" schlug er vor, eine Gegenbewegung zur rechtsextremen Trollerarmee „Reconquista Germanica" anzulegen. Trollen: Fakekonten in sozialen Netzwerken. Inhalt des Cybermobbings aus den USA: *„Kill the faggot" – „Bring die Schwuchtel um".* Der Moderator ist ein Top-Influencer mit mehr als zwei Millionen Followern bei Twitter und wurde zum Ziel von rechtsextremen Trollfabriken/Obertrollen.

3.12. Passwortsicherheit

Ein sicheres Passwort setzt sich aus einer Kombination von Ziffern, Buchstaben in Groß- und Kleinschreibung sowie Sonderzeichen zusammen.

3.13. Cyberwar, Cyberwaffen, Krieg im Cyberspace, E-Waffen (Internetangriffsmethoden)

Cyberkrieg ist eine kriegerische Auseinandersetzung im virtuellen Raum (Cyberspace) mit Mitteln der Informationstechnik. Hochtechnisierte Formen des Krieges, die auf einer weitgehenden Computerisierung, Elektronisierung und Vernetzung fast aller militärischen Bereiche basieren. Einsatzmöglichkeiten: Informationskrieg auf die Zivilbevölkerung (Flugblätter früher), Fake News, Kampagnen auf Bloggs, um Hass und Misstrauen aufzuhetzen, Desinformationsnetzwerke, Cyber-Terrorismus, Spionage, Sabotagen und materielle Angriffe (Ausschalten, Zerstören, Lähmung des Gegners übers Internet – E-Waffen: sehr billig, lassen sich global einsetzen, die Urheber operieren völlig anonym. Der Cyberspace ist nicht nur einfach ein weiterer Schauplatz, er ist überall, betrifft alle Sphären, egal ob militärisch oder zivil, man kann das ganze Land „abschalten" (Energiewirtschaft, Kommunikationen, Verkehr…). Diskussion über die chinesische Firma Huawei bzw. über die sogenannte Troll-Armee oder Putinbots (Trollfabrik, Web-Brigaden) – eine verdeckte Organisation in Russland, die im Auftrag des Staates Manipulationen im Internet z.B. mithilfe von fingierten Identitäten betreibt und die Stimmung in Online-Foren im Sinne der russischen Interessen beeinflusst (Brexit,

Trump, rechtsradikale Parteien in der EU usw.). Man vermisst eine Cyberkonvention (wie die Genfer Konvention z.B. gegen die Giftgasattacken, so eine Genfer Konvention für den Cyberkrieg – z.B. die Rechner von Krankenhäusern, Altenheimen oder bei der Flugsicherung dürfen nicht angegriffen werden).

3.14. „Nigerianische Briefe“

Tote oder politisch gestürzte Ausländer: Ein ausländischer Inhaber eines Bankkontos in Afrika, Asien oder auch Europa starb ohne Erben. Man bekommt das Angebot, sich als Erbe zu stellen. Wenn man es akzeptiert, bekommt man Anweisungen, dass man verschiedene Gebühren zahlen muss (Steuer, Rechtanwälte, Gerichtsgebühren usw.). Um eine höhere Glaubwürdigkeit des Fakes zu erzielen, verfälschen sie das Testament sowie alle anderen Unterlagen so, dass der Name des Gestorbenen denselben Namen hat, wie die Empfänger der Mail. Die Kinder eines gestürzten Politikers brauchen Hilfe, um das Geld zu überweisen.

Honesty and trust is what I am in quest of therefore your assurance of confidentiality and trust will be highly appreciated. I am sure you are aware that my father's wealth in different countries of the world was frozen. These runs into billions of dollars. *Please check these below to know more about my family wealth that were frozen.*

As you must have read from the above websites, my father still has lots of money stashed away in my foreign accounts. Right now, we are under strict custody and cannot do much. Until when we are free to move again, we will be able to locate these funds. The amount that is frozen is just a tip of the iceberg compared to what we still have out there which no one knows about, because they are not deposited with my family's name. If you believe you can keep this transaction confidential, and you assure me you will not abscond with the money after you receive it, please provide me with the following information so we can prepare the necessary documents which gives you the power to receive the funds. It will just be a private working agreement between us, which you must keep confidential.

Provide the following information:

1. Your complete names you use officially

2. Full Contact address

3. Telephone, including cell phone

4. Either your pic, your international Passport or Driver's license for identification

I am presently under house arrest, and all my movements and actions are monitored. I am cut off from the outside world. The Iranian government that accommodated us based on the good relationship they had with my late father, made a promise to the United Nations that they are keeping us on humanitarian ground, and will ensure that we are kept under strict custody to ensure

we do not make contacts to destabilize the new Libya government or cause any form of trouble. *We are banned from making any outside communications or financial transactions.* ***I only get limited access to use the internet through the help of one of the guards assigned to us. The amount of money involved is 25million dollars. I am willing to give you 25% of it for your assistance. The money is not illegal money. It rightfully belongs to my family.***

Your assistance is appreciated.

Your sister in distress.

Aisha Gaddafi

3.15. Dating-Agenturen Beispiel einer Internetanzeige: *Treffe eine hübsche Frau. Anklicken: http://www.dating88.com.* Überschriften: *Tausende von reifen Frauen suchen Liebhaber! 100% freier Zugang, aber nur heute! Diese Seite kann geheime Fotos von jemandem enthalten, den Sie kennen. Wir haben mehr als 50 000 heiße weibliche Mitglieder auf unserer Website, die gehen Späß und einfach sind. Finden Sie eine Frau und treffen Sie sich wie verrückt! Beantworten Sie ein paar Fragen, um zu sehen, ob Sie qualifiziert sind: Was für ein Körper magst du am liebsten? (4 Bilder) Welche Art von Frauen magst du? (asiatisch, weiß, braun, Ebenholz).* Fallbeispiel: Anastasiadate: Sektionen: Ukraine (Russland, Polen, Tschechien, Ungarn, Serbien, Bosnien/Herzegowina), Arabische Länder (Marokko, Georgien, Aserbaidschan), Asien (China, Vietnam, Indien), Lateinamerika (Kolumbien). Unterschiedliche Anlockungen: Beispiele von Kontakteinladungen beim Einloggen:

WANT TO BE YOUR WIFE. I want to find a decent man and build happy family with him. I'm here not to play. If I promise to make love to you every day? What do you say? When I see a man like you, I thank God I'm not married.)) I saw a dream about you! Do you want to know what is your role in it?)) I'm young, but i know it all ;) do you think i am beautiful enough to be your future wife? Are U afraid to be seduced by me? If I ever decide to get married, I'll look for a man like you do you want to marry me right now ?) hello my FUTURE MAN! i want us to have real relations and meeting, what you think? You , my mom and me My husband will be the happiest person, would you like to be my husband?

Fake profiles aus China (man möchte die Männer mit Reichtum anlocken), Beispiele:

My father inherit family Gold Mines and Gold Jewelry Factory *from my Grandparents,* ***my mom has her own successful International Investment Company and Beauty Spa Centers****, I have my own hotels and Spa Centers now, maybe u feel it is so amazing and can't believe it, but u will know and understand when i tell u in detail and show u around, I am not mean to show u how rich I am, just want to tell u I will not care about your material things, your age and*

your look if u secious like me, what I need most is just your serious truthful heart and true love to me. My love, I am so ready for our rest life time happy together

I am successful woman who has great cars, like Lamborghini, Benz, Ferrari*. Oneo of my favourate is collecting cars, and enjoy the rush feeling when i am on road and wind howls beside me.*

As for me, ***I have my five stars hotels in Beijing, Shanghai, Shenzhen, Zhengzhou, Hangzhou and Hongkong, i do the investment in spa centers, my parents running our jewelry business and another four hotels in HK and take good care of my younger sister who is study here****, i* ***have twenty billion to share with my future husband****.*

Have u heard of Jiayin Xu, the chairman of Evergrande Real Estate Group? He is the most rich man in China and very famous, ***I am his illegitimate daughter*** *live with my mom with no one know us, in order to protect father's reputation as a famous successful man, we need to hide this secret and live apart from him, what he give us is just money and comfortable rich life.*

Fazit: *„Wir brauchen eine neue Informationsethik. Die müssen wir entwickeln, anstatt die alten Regelwerke immer wieder mit neuen Software-Updates zu überarbeiten. (...) Die Atombombe können nur relativ wenige Länder herstellen. Digitalwaffen dagegen könnten theoretisch von einem Teenager mit einem Laptop missbraucht werden. Es gibt derzeit nur eine Möglichkeit, einen Computer gegen Missbrauch zu sichern. Stecker ziehen, in Beton gießen und auf dem Meeresgrund versenken"* (Luciano Floridi, Der Spiegel 8/2015, S. 120).