Computerprävention

Sensibilisierung für Gefahren im Netz

Von EKHK a.D. Klaus Kemper, Duisburg[1]

1 Allgemeines

Ende der 1990er-Jahre setzte sich in der deutschen Polizei die Einsicht durch, dass es dringend geboten sei, neben der Strafverfolgung auch der Kriminalprävention in Form eigener Organisationseinheiten einen höheren Stellenwert einzuräumen. Neben den bereits seit Jahrzehnten durchgeführten sicherheitstechnischen Hinweisen zur Vermeidung von Einbruchsdiebstählen wurde in diesen Dienststellen nun auch verstärkt auf die Verhaltensprävention im Zusammenhang mit den Bereichen Rauschgift-, Gewalt- und Jugendkriminalität sowie Sexual- und Betrugsdelikte gesetzt. Nachdem um die Jahrtausendwende Computer sowie das Internet praktisch für jeden Bürger verfügbar geworden waren, dauerte es nicht lange, bis die ersten Anwender auch die sich ihnen bietenden Möglichkeiten dieser technischen Errungenschaften nutzten, um mit ihnen Straftaten zu begehen. Diese mittels Anwendung der Informations- und Kommunikationstechnik, kurz IuK, durchgeführten Delikte werden unter dem Oberbegriff „Computerkriminalität“ oder auch „Cybercrime“ zusammengefasst und haben in den letzten zwei Jahrzehnten einen enormen Aufschwung erlebt. Laut der Polizeilichen Kriminalstatistik des BKA für das Jahr 2020 wurden in diesem Zeitraum 130.611 Fälle bekannt, was einen Anstieg von 7.605 Fällen bzw. ein Plus von 6,2% bedeutet.[2] Da sich diese Entwicklung verhältnismäßig frühzeitig abzeichnete, wurden die bekannt gewordenen Modi Operandi auch recht zügig in das Portefeuille der kriminalpolizeilichen Vorbeugungsmaßnahmen aufgenommen und die Sachrate „Computerprävention“ geschaffen.

2 Persönliche Daten

Die persönlichen Daten jedes einzelnen Menschen können für andere Privatpersonen, Institutionen oder Firmen für ihre eigenen Zwecke von großem Interesse sein. Sie geben nicht nur Aufschluss über Namen, Geburtsort und -datum sowie Wohnanschrift, sondern ermöglichen Interessierten auch einen Blick auf Vorlieben, Kaufgewohnheiten oder Bewegungsbilder. Um dies zu vermeiden, sind die Persönlichkeitsrechte in der Bundesrepublik seit Jahren durch entsprechende Datenschutzgesetze und -verordnungen, z.B. das Bundesdatenschutzgesetz (BDSG), geschützt. Während in der gesamten Europäischen Union entsprechende rechtliche Bestimmungen gelten, hat in den USA nach den terroristischen Anschlägen im Jahr 2001 der sog. „Patriot Act“ die diesbezüglichen Rechte der Bürger in bestimmten Situationen eingeschränkt.

3 Erschleichen von Daten und deren Missbrauch

Wie bereits angesprochen, aber auch detailliert in den vorangegangenen Beiträgen der Fachzeitschrift „Die Kriminalpolizei“ dargelegt, hat der Missbrauch persönlicher Daten in den letzten Jahren stark zugenommen. Dabei ist zunächst festzuhalten, dass natürlich gegen deren freiwillige Preisgabe durch den Bürger nichts einzuwenden ist. Dazu ist aber die ausdrückliche Einwilligung erforderlich. Im Gegensatz zu Deutschland nehmen es viele andere Länder mit dem Datenschutz weniger genau,

dort hat sich mittlerweile ein regelrechter Markt für diese „Ware“ gebildet. Hintergrund ist u.a. das Interesse der Werbeindustrie, auf diese Weise an Personenprofile zu gelangen. Diese helfen dann dabei, die Bürger per Internet oder auf andere Art mit auf sie zugeschnittener Werbung zu konfrontieren. Ist dieses Vorgehen für die Betroffenen eher lästig, so sind andere (strafbare) Handlungen im Zusammenhang mit persönlichen Daten oft auch mit finanziellem Schaden verbunden. Dabei wurde diesbezüglich auch schon vor dem „Computer-Zeitalter“ auf Möglichkeiten der Telekommunikation zugegriffen. So köderten Straftäter per Telefon arglose, häufig betagte Bürger mit angeblich bei Gewinnspielen für sie ausgelosten Preisen, ihre persönlichen Daten preiszugeben. Mit gezielt gestellten Formulierungen, die zwangsläufig ein zustimmendes „ja“ beim Angerufenen hervorlockten, wurde diesen dann, ohne dass sie es wussten, z.B. ein Zeitschriften-Abonnement „untergejubelt“. Exemplarisch sei hier auch noch der „Enkeltrick“ erwähnt, bei dem der Anrufer zunächst durch geschickte Fragen an persönliche Daten aus dem familiären Umfeld eines kontaktierten Senioren gelangt. Mit diesen wird dann die Notlage eines Enkels oder anderen Verwandten vorgetäuscht und der Senior zum Abheben einer bestimmten Geldsumme bewegt, die dann einem Boten des vermeintlich in Not geratenen Familienmitglieds übergeben werden soll. Mit dem Einzug des Computers in den Alltag der Bürger wurde die Palette der damit verbundenen kriminellen Möglichkeiten erheblich erweitert, wobei diese zum Großteil im Zusammenhang mit bekannten Straftatbeständen, wie z.B. dem Betrug, stehen. Die Aufgabe der Sachrate Computerprävention besteht darin, die Öffentlichkeit über die entsprechenden Modi Operandi zu informieren und Möglichkeiten aufzuzeigen, wie man vermeidet, Opfer derartiger Delikte zu werden. Im Folgenden sind einige der gängigen Arten von Malware ebenso aufgeführt wie Hinweise, sie als solche zu erkennen.

3.1 Spyware

3.1.1 Phishing

Grundsätzlich ist die Datenweitergabe durch Dritte nicht strafbar, sofern die Einwilligung dazu vorliegt. Strafbar ist sie allerdings, wenn sie ohne eine solche durchgeführt wird, um damit dann Aktionen durchzuführen, durch die der eigentliche Eigentümer geschädigt wird. Im Zusammenhang mit den Möglichkeiten des Internets ist nicht einmal ein wie auch immer gearteter direkter Kontakt zwischen den Parteien vonnöten. Es bedarf lediglich der geschickten Täuschung, die den eigentlichen Nutzer, meist per E-Mail, zur Herausgabe seiner Daten, bevorzugt z.B. seiner Kontonummer oder ähnlicher sensibler Informationen, veranlasst. Dazu bedient der Täter sich oft angeblich seriöser Einrichtungen, wie z.B. Geldinstituten oder Telefonanbietern, die aufgrund sich ergebender Notwendigkeiten um die Übersendung der benötigten Angaben bitten. Im Erfolgsfall wird den Opfern dann in der Regel ein finanzieller Schaden zugefügt, da nun auf deren Konto zugegriffen werden kann. Diese Praxis wird als „Phishing“ bezeichnet, einem dem englischen „fishing“ (fischen) nachempfundenen Begriff. Die Gefahr, Geschädigter einer solchen Cyber-Attacke zu werden, reduziert sich erheblich, wenn der angeschriebene User die folgenden Hinweise beherzigt:

> Auch wenn die im Anschreiben niedergelegte E-Mail-Adresse aufgrund früherer Kommunikationen bekannt scheint, sollte sie noch einmal eingehend geprüft werden. Hintergrund ist die Tatsache, dass sich verschiedene Buchstaben in den möglichen Computerschriften verwechseln lassen. Als Beispiel seien hier der Kleinbuchstabe l (Calibri) und der Großbuchstabe I (Arial) genannt. Darüber hinaus sind auch die Null und der Großbuchstabe O schnell zu verwechseln.
>
> Zip-Dateien werden generell nicht im Zusammenhang mit Zahlungsaufforderungen verschickt.
>
> Meist wird der Adressat nicht direkt angesprochen, sondern mit den allgemeinen Floskeln „sehr geehrter Kunde“ oder „sehr geehrte Damen und Herren“, eine Praxis, die in echten Schreiben in der Regel nicht verwendet wird.
>
> Die E-Mails beinhalten oft Grammatikfehler oder fragliche Redewendungen, was darauf hinweisen kann, dass sie mit Hilfe eines Übersetzungsprogramms erstellt worden sind. Derartige Formulierungsprobleme finden sich niemals in tatsächlichen Benachrichtigungen von Kreditinstituten oder seriösen Firmen.
>
> Enthält das eingegangene Schreiben den Hinweis auf eine gewisse zeitliche Dringlichkeit der erbetenen oder gar geforderten Maßnahme, besteht der Verdacht einer Phishing-Mail.
>
> Eine weitere Möglichkeit, sich über die Echtheit des Anschreibens rückzuversichern, besteht im Vergleich der angeblichen E-Mail-Adresse des Absenders mit dessen tatsächlicher elektronischer Erreichbarkeit.
>
> Auch der Griff zum Telefon zwecks fernmündlicher Rücksprache mit einem Sachbearbeiter bringt Klarheit, inwieweit die Benachrichtigung der Wahrheit entspricht.
>
> Bei Bewerbungen auf Ausschreibungen ist es ratsam, in den zu übersendenden Unterlagen zunächst keine Kontodaten oder Kopien von Personalpapieren mitzuschicken. Das kann auch zu einem späteren Zeitpunkt erfolgen, wenn die Seriosität des Gegenübers feststeht.

3.1.2 Spear-Phishing

Beim „Spear-Phishing“ handelt es sich um eine Abwandlung des Phishing, bei dem bestimmte Personengruppen, z.B. Studierende einer Universität, gezielt von einem angeblich ortsansässigen Geldinstitut angeschrieben werden. Die Wahrscheinlichkeit, dabei tatsächliche Kunden zu erreichen, liegt so höher als bei wahllos auf den Weg gebrachten E-Mails. Entsprechend wünschenswert ist ein flächendeckender Hinweis der jeweiligen Einrichtung an ihre Mitglieder auf die Gefahr, Opfer dieses kriminellen Ausspähversuches zu werden. Neben der Beherzigung vorgenannter Hinweise bietet auch darauf ausgerichtete Hardware nachhaltigen Schutz gegen derartige und ähnlich gelagerte Phishing-Angriffe. Exemplarisch sei hier noch das „Pharming“ genannt, bei dem die DNS-Anfragen von Webbrowsern, z.B. durch DNS-Spoofing, so manipuliert werden, dass der User auf gefälschte Websites umgelenkt wird. Darüber hinaus können die Bürger sich natürlich auch bei den Fachberatern der Kriminalpolizeilichen Präventionsdienststellen informieren.

3.2 Ransomware

Wurden bei den bisherigen Betrachtungen Straftaten in den Vordergrund gestellt, die durch Erschleichen persönlicher Daten des Bürgers mittels Internet diesen finanziell schädigen, soll auch auf eine andere, „Ransomware“ genannte Art der Malware eingegangen werden. Dabei gelingt es dem Kriminellen, den User dazu zu bewegen, eine bestimmte infizierte Seite zu öffnen, durch die dann ein Schadstoffprogramm bei ihm aufgespielt wird. Dies kann durch gezielte Täuschung, versehentlich oder auch aus Neugier geschehen. Danach ist ein Zugriff auf das Gerät in der Regel nicht mehr möglich. Erst nach Zahlung eines Lösegelds werden die Daten wieder freigegeben. Da, insbesondere auf dem wirtschaftlichen Sektor, im Falle eines Verlustes von Geschäftsdaten oder anderer wichtiger Informationen schwere finanzielle Einbußen die Folge sein können, wird dringend geraten, sich entsprechende Antivirenprogramme auf den Computer aufzuspielen.

4 Kinder und Jugendliche im Netz

Die meisten der Kinder und Jugendlichen in der heutigen Zeit sind wie selbstverständlich mit dem Computer und den sich damit ergebenden Möglichkeiten aufgewachsen. Natürlich ist es den jeweiligen Erziehungsberechtigten überlassen, inwieweit sie die Zugriffe ihrer Sprösslinge auf dieses Medium dulden bzw. beschränken. Es ist eine erfreuliche Tatsache, dass die mit dem Thema Computerprävention befassten Polizeibeamten immer wieder in Lehrerkonferenzen oder Elternversammlungen, aber auch zu Thementagen eingeladen werden, um dort die Möglichkeiten der dort anwesenden Personengruppen, ihre eigenen oder die ihnen anvertrauten jungen Menschen vor den möglichen Gefahren des Internets zu bewahren, darzulegen. Dabei ist die Erklärung der jeweiligen Modi Operandi von nicht unerheblicher Bedeutung. Nachfolgend soll kurz auf die häufigsten Delikte im Zusammenhang mit Minderjährigen eingegangen werden:

4.1 Soziale Netzwerke

Viele Kinder und Jugendliche haben Freude daran, sog. Soziale Netzwerke zu nutzen und sich in ihnen mit Gleichaltrigen über für diese Altersgruppen typische Themen auszutauschen. Dabei werden oft auch persönliche Daten preisgegeben sowie Bilder verschickt. Dies geschieht meist arglos und ohne daran zu denken, dass grundsätzlich auch die Gefahr besteht, dass andere, dem Absender unbekannte Personen, über welche Wege auch immer, an diese Angaben oder Fotografien gelangen und diese dann eventuell missbräuchlich verwenden können. Das kann später möglicherweise zu Unannehmlichkeiten für den betroffenen Minderjährigen führen, die er niemals in Erwägung gezogen hat. Aus diesem Grund, aber auch im Zusammenhang mit noch weiter aufgeführten Gefahren im Netz, wird Eltern, Lehrkräften sowie anderen Vertrauenspersonen der Kinder und Jugendlichen geraten, ihre Schutzbefohlenen auf solche Aktivitäten hinzuweisen und sie davon zu überzeugen, dass sie stets als vertrauensvolle Gesprächspartner zur Verfügung stehen. Im oben genannten Fall ist es z.B. wichtig, den jungen Menschen klar zu machen, dass sie möglichst wenig von sich preisgeben und sichere Passwörter wählen sollen, aber auch, dass sie selbst, etwa durch das Verwenden von Lichtbildern Anderer, im Sinne des Urheber- und Persönlichkeitsrechts in einen strafbaren Bereich geraten können.

4.2 Cybermobbing und -grooming

Im Zusammenhang mit den unter 4.1 aufgeführten Fakten muss auch auf die Phänomene Cybermobbing und -grooming hingewiesen werden. Im ersten Fall werden junge Menschen, meist anonym, mittels in sozialen Netzwerken veröffentlichten Beschimpfungen, anderer Unflätigkeiten oder ungünstigen Fotos verunglimpft, was für diese Person oft zu schweren psychischen Belastungen bis hin zu weiteren Folgen wie Depression oder gar Suizidgedanken führen kann. Beim Cybergrooming wiederum versuchen Erwachsene, Kontakt zu Kindern oder Jugendlichen aufzubauen mit dem Ziel, ihre Opfer letztlich persönlich zu treffen, sie möglicherweise zu sexuellen Handlungen zu bewegen. Dies kann, selbst wenn es beim Versuch bleibt, beim Betroffenen zu schweren seelischen Schäden führen. Selbstverständlich gelten auch hier die im vorhergegangenen Unterpunkt benannten Verhaltenshinweise, verbunden mit dem sofortigen Abbruch der Chats sowie einer Strafanzeige.

4.3 „Abzocke“ im Internet

Auch im Internet sind Betrüger unterwegs, die versuchen, User um ihr Geld zu bringen. Dabei lassen sich oft auch surfende Minderjährige dazu verleiten, auf verlockende Angebote hereinzufallen. Exemplarisch sei hier die scheinbar kostenlose Teilnahme an Gewinnspielen genannt, bei der sich hinterher herausstellt, dass dies keineswegs so ist. Hat der junge Mensch sich als volljährig ausgegeben und die AGB anerkannt, flattert dann eine Rechnung ist Haus, die meist so spät kommt, dass auch das Widerrufsrecht abgelaufen ist. Ebenso mit Vorsicht zu genießen sind besonders verlockende Verkaufsangebote, gerade wenn deren Lieferung gegen Vorkasse erfolgen soll. Oft geht die Ware danach beim Käufer niemals ein. Bezüglich dieser Betrugsmaschen sollte den jungen Menschen verdeutlicht werden, dass solche Angebote immer mit der gebotenen Skepsis zu betrachten sind und nie per Vorkasse bezahlt werden sollten, wobei auch Nachforschungen in Diskussionsforen häufig weitere Klarheit bezüglich der Seriosität des Verkäufers bringen können.
Über die angesprochenen Themen hält neben den polizeilichen Beratungsstellen auch das überörtliche ProPK (Programm Polizeiliche Kriminalprävention) unter dem Titel „Klicks-Momente“ Informationsmaterial für interessierte Bürger bereit.[3]

Anmerkungen

1. Der Autor war als EKHK Leiter der Kriminalkommissariats für Kriminalprävention und Opferschutz (KK KP/O) beim Polizeipräsidium Duisburg.
2. PKS BKA für 2020, S. 22.
3. www.polizei-beratung.de/gefahren-im-internet.