Experimentierfeld Polizei:
Von Alpha bis Omega

Interview:
10 Fragen an Mag. Löschl

Technik:
Waffe aus 3D Drucker

05/12

kripo.at

VEREINIGUNG KRIMINALDIENST ÖSTERREICH

Digitaler Tatort

"Mit List und Tücke"
Die neue kripo.at-Broschüre ist da!
mehr auf Seite 19

Verlagspostamt 8073 Feldkirchen bei Graz P.b.b. Zulassungsnummer 03Z035266M - € 4,-

Tatortarbeit in Zeiten von Smartphone und Tablets

Ein wenig Nostalgie gefällig? Was waren das für herrliche Zeiten, als man bei einer Hausdurchsuchung wusste, was man suchen muss. Das gestohlene Autoradio, das Tatwerkzeug – man sah es und stellte es sicher. Selbst bei Betrügern, denen meine besondere dienstliche Aufmerksamkeit galt, konnte man anno dazumal, also bis ins Jahr 2000, Materielles vorfinden – die getrickste Buchhaltung, die damals noch aus Papier bestand, ein gefälschter Ausweis und und und!

Die Zeiten haben sich geändert. Wie mir aus glaubhafter und bestens informierter Quelle berichtet wird, müssen die amtshandelnden Kollegen heute häufig nach unsichtbaren Dingen suchen. Schon klar, gesucht werden Beweismittel gegen einen Kriminellen, nur was dies sein könnte und hinter welcher Fassade es sich verbirgt, das ist heute im Vorfeld kaum bekannt. Beweismittel sind heute häufig nicht materieller, sondern digitaler Natur und damit vorerst unsichtbar. Die Spezialisten, die aus digitalen Daten sichtbare Informationen herauslesen können, sind auch nur einsetzbar, wenn der Beamte vor Ort das richtige Speichermedium ohne Datenverlust sicherstellt. Die Betonung liegt auf „ohne Datenverlust“. Soll man also den Computer abdrehen oder eingeschaltet sicherstellen? Das ist ja noch eine einfache Frage, die Schwierigkeiten beginnen hier aber erst.

Unglaublich aber wahr, heute hinterlassen nur dumme Kriminelle auf ihrem Computer Spuren ihrer Straftat. Wenn die Polizei vor der Türe steht, lässt sich ein inkriminierender Computer nicht mehr durch die Klospülung oder über das Fenster entsorgen. Die Lösung heißt CD, DVD oder Stick. Diese kleinen Dinger sind schon viel schwerer zu finden. Und wer unter 100 CDS eine belastende versteckt, hat gute Chancen, dass diese nicht entdeckt zu werden. System „Nadel im Heuhaufen“, nein besser „Nadel im Nadelkissen“. Als in Polizeikreisen auch dieses Schlupfloch bekannt war, machten sich die Kriminellen sofort die neueste technische Entwicklung zu Eigen. Heute lagern die vifen Täter ihre Daten im cloud aus.

Sie wissen nicht, was „cloud“ heißt? Sie wissen nicht, was man bei der Sicherstellung eines Smartphones, eines Computers tun muss? Nun das mindeste ist, die Artikel über das Thema in dieser Ausgabe zu lesen.

Wenn Ihnen das nicht genügt, wir können Ihnen weiterhelfen, denn die VKÖ fördert Fortbildung und veranstaltet Anfang 2013 ein entsprechendes Seminar. Wir sind nämlich der Meinung, dass jeder Polizeibeamte grundsätzlich wissen sollte, wie er beim ersten Angriff einen digitalen Tatort absichern kann.

Richard Benda
Präsident

INHALT

NEWS

Nationale und internationale Short-Cuts

USA: Datenmissbrauch: falsche Standorte

Eine Facebook-Nutzerin aus Boston hat festgestellt, dass auf ihr Konto aus Orten, die mehr als 600 Kilometer entfernt sind, mehrmals zugegriffen wurde. Es gibt auf Facebook eine Reihe von Diensten, die den Aufenthaltsort der Anwender feststellen und für Werbemaßnahmen verwenden. Diese Dienste sind viel zu intransparent.

So wurde vor allem in den USA festgestellt, dass in den entsprechenden Protokollen Zugriffe aus weit entfernten Orten verzeichnet sind. "Auf Anfrage eines Journalisten antwortete Facebook, wie meist, unkonkret. "Wir nutzen Informationen von Mobilfunkbetreibern und den Endgeräten unserer Nutzer. In manchen Fällen können wir den Nutzer aber nicht genau orten. Deswegen wird ein beliebiger Standort angezeigt", erklärt Facebook-Sprecher Frederic Wolens.

Facebook gibt also offiziell zu, dass Standorte seiner Nutzer festgestellt werden. Es ist aber sehr problematisch, dass die Daten inkorrekt sind. "Die Informationen werden für Geo-Marketing verwendet, dadurch kann lokale Werbung angezeigt werden". Facebook versucht damit endlich an Geld zu kommen.

DEUTSCHLAND: Streit um Staatstrojaner

EDer bayerische Datenschutzbeauftragte Petri fordert "Trojaner-Gesetze" für Bund und Länder. Diese seien notwendig, um den Einsatz der Spionage-Software zur sogenannten Quellen-Telekommunikationsüberwachung durch die Polizei zu regeln, sagte er nach einer Überprüfung von Maßnahmen zum Abhören der Internet-Telefonie. Der Jurist sprach von einem "tiefdunklen Graubereich", in dem die bayerischen Strafverfolger agiert hätten. Bei der eigenen Landesregierung ist Petri mit seiner Forderung auf taube Ohren gestoßen. Der bayerische Innenminister Joachim Herrmann will die Hinweise des Landesbeauftragten nach eigenen Angaben zwar "sorgfältig prüfen und sie bei der datenschutzgerechten Fortentwicklung der Software zur Quellen-TKÜ einbeziehen". Der Politiker sieht aber "keinen zwingenden gesetzgeberischen Bedarf", Einzelheiten zur Verwendung von Staatstrojanern festzulegen. Er stellt fest, dass die umstrittene Maßnahme in der Strafprozessordnung (StPO) ihre Rechtsgrundlage findet.

ENGLAND: Cyberangriff auf britische Polizei

Hacker sind kürzlich in das Netzwerk der britischen Polizei eingedrungen und haben Zugriffsdaten von Dutzenden Beamten erbeutet und später auch veröffentlicht. Die Hertfordshire Police hat den Vorfall bestätigt und teilt mit, dass die Daten, darunter IP-Adressen und Telefonnummern, von einem externen Netzwerk gestohlen wurden. Die betroffenen Seiten wurden vom Netz genommen und die Sicherheitsbehörden sind um Aufklärung bemüht.

"Bislang gibt es keinen Hinweis darauf, dass persönliche Daten von Polizeibeamten oder anderen Personen missbraucht werden könnten", so die britische Polizei in einer Stellungnahme.

Der Vorfall kommt sehr ungelegen, denn die EU hat unlängst die Errichtung einer zentralen IT-Sicherheitsbehörde beschlossen, in der 30 Experten gegen die organisierte Cyberkriminalität vorgehen sollen. Die neue Einrichtung soll 2013 starten und jährlich 3,6 Mio. Euro kosten.

INTERNATIONAL: Große Probleme bei Datenvernichtung

Während fast drei Viertel der Unternehmen einen Aktenvernichter oder Shredder für alte Dokumente haben, besitzen nur 40 Prozent eine professionelle Lösung zur Vernichtung elektronischer Daten. Nur eine Minderheit der Betriebe hat eine tatsächliche Regelung für die Entsorgung von IT-Altgeräten.

Nicht richtig gelöschte Daten beschäftigen schon seit Jahren die Öffentlichkeit. Dies vor allem wenn bekannt wird, dass wichtige Datenträger von Behörden oder der Alt-Rechner eines Sachbearbeiters inklusive vermeintlich gelöschter, vertraulicher Daten auftauchen.

Ein weiterer potenzieller Stolperstein ist, dass eine Datenlöschung nur über die integrierten Funktionen von IT-Geräten meist nicht sicher ist. Bei einer Festplatte zum Beispiel sind Daten, wenn sie normal gelöscht werden, nicht verschwunden. Sie werden nur zum Überschreiben freigegeben und sind im Inhaltsverzeichnis nicht mehr sichtbar. Experten können in solchen Fällen normalerweise einen Großteil der Daten wiederherstellen - was bei unbeabsichtigter Löschung gut, aber bei der Geräteentsorgung ein Risiko ist.

Wie schnell können Beweise verloren gehen?

Die Sicherung von digitalen Spuren ist der erste und gleichzeitig kritischste Schritt bei der Durchführung einer digitalforensischen Untersuchung. Erfahrungsgemäß ist die Datensicherung der Prozess, bei dem die meisten unumkehrbaren Fehler passieren können. So könnten z.B. unbeabsichtigte Schreibzugriffe auf dem zu analysierenden Datenträger erfolgen. Dadurch würde man einen erheblichen Schaden auf dem Speichermedium verursachen, da eventuell zu rettende Daten im schlechtesten Fall unwiederbringlich gelöscht wären. Abgesehen davon, ist im Hinblick auf den klassischen forensischen Prozess jegliche Integrität der Daten zu bewahren, um Vorwürfen der Manipulation von Beweismitteln vorzubeugen.

Eine professionelle und gerichtsverwertbare Datensicherung kann bei der Frage nach der Zulässigkeit eines Beweismittels vor Gericht von entscheidender Bedeutung sein. Darüber hinaus bestärkt eine fachmännisch durchgeführte Sicherung die Glaubwürdigkeit vor Gericht. Noch kritischer zu betrachten ist die Sicherung von flüchtigen Daten, wie dem Inhalt des Arbeitsspeichers. Fehler in diesem Stadium werden erbarmungslos bestraft. Diese Bits und Bytes leisten für die spätere Auswertung einen wertvollen Beitrag. So können sie beispielsweise Passwörter beinhalten, die nirgends sonst auf herkömmlichen Datenträgern gespeichert sind.

Findet ein Ermittler vor Ort einen Verdächtigen Computer vor, sollte es die erste Aufgabe sein, diesen "virtuellen Tatort" abzusperren, damit keine fremde Person mehr Zugriff auf dieses System hat. Der „virtuelle Tatort“ ist dabei genauso sensibel zu betrachten, wie ein realer Tatort. Auf einem Computer befinden sich ebenfalls zahllose verschiedenste Spuren, die vor jeglichen weiteren, zerstörerischen Einflüssen geschützt werden müssen. Für eine spätere Auswertung und Nachweisbarkeit im Ermittlungsprozess stellen die Zeitstempel (MAC-Times genannt) wichtige Indizien dar. Diese Zeitstempel geben Auskunft darüber, wann jemand eine Datei erstellt, geändert oder gespeichert hat.

Trifft ein Ermittler auf ein noch laufendes Computersystem, gibt es besondere Sorgfalt walten zu lassen. Gerade im Zeitalter von Verschlüsselungen, Clouds, Netzwerkverbindungen, Informationen über angemeldete Benutzer (User-Accounts), usw., ist es immer wichtiger, so viele Informationen wie möglich im noch laufenden Zustand zu sichern. Es gibt eine große Anzahl an verschiedenen Verschlüsselungstools, die frei aus dem Internet herunter geladen werden können. Eine solche Verschlüsselung mit sogenannten Passwortattacken (Brute-Force-Attacken) zu umgehen, ist schwierig, zeitintensiv bis gar unmöglich.

Immer beliebter sind die so genannten Cloud-Lösungen. Bei einer Cloud handelt es sich um einen gemieteten externen Festplattenspeicher. Diese Speicherkapazitäten werden meist von Internetdienstanbietern mit zur Verfügung gestellt. Der Benutzer baut über das Internet eine verschlüsselte Datenverbindung (VPN) auf und kann diesen externen Speicher wie eine Festplatte auf seinem Rechner einbinden und genauso nutzen. Auch hier können mit einem einfachen Bildschirmfoto schon wertvolle Hinweise auf das Vorhandensein einer Cloud dokumentiert und gesichert werden. Darüber hinaus befinden sich auch hier wiederum wertvolle Informationen im Arbeitsspeicher, die für eine spätere intensive Auswertung von großer Bedeutung sein können. Ein namhafter Mobiltelefonhersteller macht derzeit für diese Lösung viel Werbung und zeigt die vielen Möglichkeiten eines solchen Speicherplatzes auf, der auch von überall aus erreichbar ist.

Das größte Problem stellt meist der Mensch selbst dar, nämlich dann, wenn er eine Situation falsch einschätzt oder unterschätzt. Zu glauben, einfach den Stecker zu ziehen, alles einzupacken und dann die Kollegen von der Auswertung damit beschäftigen zu lassen, wäre mit einer der schlimmsten Fälle. Anhand dieser kleinen vorgenannten Beispiele, ist schon erkennbar, dass es bei einem Computer um einen sehr sensiblen Tatort handelt, der jegliche

falsche Handhabung erbarmungslos bestraft. In einem Arbeitsspeicher befinden sich zahlreiche Informationen, die bei einer Stromunterbrechung (Stecker ziehen) unwiderruflich verloren gehen.

Auch das normale Herunterfahren eines Computers, kann versteckte Löschroutinen, wie z. B. das Löschen von temporären Dateien oder die Veränderung von Zeitstempeln auslösen. Wenn man bedenkt, dass bei einem normalen Windows-Start ca. 1000 Zeitstempel verändert werden, ist das eine ganz Menge Daten, die dabei verloren gehen.

Selbstverständlich sind die Fähigkeiten eines „Otto-Normalverbrauchers“ in Bezug auf die hier notwendige Sach- und Fachkunde beschränkt. Dennoch gibt es erlernbare Schemata, die durch jedermann angewendet werden können. Die simpelste Variante besteht darin, eine lückenlose Dokumentation durchzuführen. Jeglicher Eingriff, dazu zählt auch schon das einfache Bewegen einer Computermaus, muss durch den Ermittler exakt protokolliert werden. Dazu empfiehlt sich der Abgleich von der angezeigten Systemzeit mit der Realzeit.

Werden bei den ersten Maßnahmen Fehler begangen, kann dieses zur Folge haben, dass die Beweiskette gebrochen wird und ein Beweismittel (z. B. Festplatte) nicht mehr in ein Gerichtsverfahren eingebracht werden kann. Somit steht vielleicht das einzige Beweismittel nicht mehr zur Verfügung.

Gerade die Aufklärung im Bereich der Computerkriminalität ist äußerst schwierig. Laut Statistik des Bundeskriminalamtes in Deutschland (BKA, Polizeiliche Kriminalitätsstatistik 2011) kann nur etwa ein Viertel der Straftaten aufgeklärt werden. Die Computerkriminalität entwickelt sich immer weiter und wird in ihren Erscheinungsformen immer vielfältiger. Nur wenn von Beginn an die richtigen Schritte eingeleitet werden, besteht überhaupt die Möglichkeit, diese Straftaten aufzuklären.

Verfasser: Andreas Bauer, CEO, Verband Europäischer Gutachter & Sachverständiger (VEGS).

Fahndung nach Twitter-Psychopathen

Sie verwenden Wörter wie "stirb","töten", oder "begraben", jene Twitter Psychopathen, welche immer wieder im Netz auftauchen und für Unruhe und Ängste bei vielen Benützern sorgen. Forscher der Florida Atlantic University haben ihnen den Kampf angesagt und eine Methode entwickelt, mit der sie aufgrund von Twitter-Nachrichten feststellen können, ob Nutzer des Microblogging-Dienstes Psychopathen sind.

Für die Studie wurde die Wortwahl von 3.000 Twitter-Nutzern analysiert. Die Wissenschaftler gehen davon aus, dass bestimmte Ausdrücke auf einen tendenziell psychopathischen Charakterzug hinweisen. Diese neue Methode könnte schon bald im Gesetzesvollzug zum Einsatz kommen.

Dieses Analyseverfahren soll einerseits der Verbrechensvorbeugung dienen und andererseits Arbeitgebern Einblick in die Psyche potenzieller Mitarbeiter gewähren. Für die Studie wurde eine Formel angewendet, die in der Kriminologie bereits jetzt erfolgreich eingesetzt wird. Der Algorithmus durchsuchte die Tweets ((englisch to tweet = zwitschern) der Personen, die freiwillig an der Studie teilgenommen haben. Dabei kam man zum Ergebnis, dass 1,4 Prozent aller Teilnehmer psychopathische Neigungen zeigen.

Mögliche Konflikte

Die Forscher gehen davon aus, dass dies ein Indikator für Psychopathie ist. Hundertprozentige Resultate gibt es allerdings noch nicht. Studien über die Verbindung von Sprache und der mentalen Gesundheit von Menschen wurden schon oft erstellt und zur Kriminalprävention verwendet. Neu ist, dass in dieser Studie zum ersten Mal auch soziale Medien unter die Lupe genommen wurden.

Bevor das Analyse-Werkzeug zur Verbrechensbekämpfung eingesetzt werden kann, sind noch einige wissenschaftliche Arbeiten erforderlich.

Dennoch sind die Forscher von dem neuen Verfahren überzeugt, wohl wissend, dass es noch nicht perfekt ist. Darüber hinaus fürchten sie, dass es zu möglicherweise zu Konflikten mit Datenschützern kommen könnte. Dem gegenüber steht allerdings die Verantwortung des Einzelnen, was er im Netz preisgibt.

Kritik

Kritik kommt von Experten. Der ärztliche Leiter der Justizanstalt Göllersdorf/NÖ hält die These der Forscher für absurd. "Wenn ich über einen Mord schreibe, werden Wörter wie töten sehr oft vorkommen. Es kommt immer auf den Kontext an". Der forensische Psychiater ist daher von der Studie keineswegs überzeugt. und spricht von "Menschen, die sich in den Medien wichtig machen wollen".

Die Methode, welche im Dezember bei der International Conference of Machine Learning and Applications vorgestellt werden soll, hat grundlegende Einschränkungen, die sich auf das Resultat auswirken. Das Verfahren kann abgekürzte Wörter, die auf Twitter sehr häufig sind, nicht erkennen. Außerdem werden die Emotionen der Nutzer nicht berücksichtigt.

• Josef W.Lohmann

10 kripo.at FRAGEN AN

Mag. Leopold Löschl

Leiter des Büro 5.2
Computer- und Netzwerkkriminalität

"Potential der Täter wird sich rasant vergrößern"

kripo.at: Herr Mag. Löschl, Ihr Büro ist innerhalb der Polizei unter den Namen C4 (Cybercrime Competence Center) bekannt. Was macht Ihre Abteilung eigentlich?

Mag. Löschl: Unser Büro ist für Computer- und Netzwerkkriminalität zuständig. Das heißt wir sind für die forensische Beweissicherung sowohl am PC als auch in Netzwerken zuständig. Stark im Ansteigen ist die mobile Forensik. Darüber hinaus ermitteln wir in manchen Fällen auch selbst. Das macht uns zu einem atypischen Assistenzdienst. Der Ermittlungsbereich umfasst Computerdelikte im Strafrecht, die sich speziell mit Daten und EDV-Systemen befassen. Es sind dies die § 118a, also das klassische Hacking, §§ 126a, b, c, die Datenbeschädigung, Angriffe auf Computersysteme, Missbrauch von Computerprogrammen, § 148a, betrügerischer Datenverarbeitungsmissbrauch und § 225a, das ist die Datenfälschung. Mittlerweile sind wir in der Umsetzungsphase des C4, was über unseren ursprünglichen Aufgabebereich hinausgeht. Wir ziehen hier selbst gewisse Delikte an uns, wie zum Beispiel den „Polizeitrojaner".

kripo.at: Die Bekämpfung von Computerkriminalität bedarf anderer Vorgangsweisen als klassische Kriminalität. Wie arbeitet Ihr Büro?

Mag. Löschl: Das hängt immer vom jeweiligen Fall ab. Wir haben einerseits die Assistenzaufgaben und die Ermittlungsaufgaben. Wir werden zu Hausdurchsuchungen beigezogen, wenn man schon im Vorfeld weiß, dass elektronische Beweismittel aufgefunden werden oder zu erwarten sind. Dann führen unsere Beamten die Sicherstellung durch. Wir stellen den aktuellen Modus der elektronischen Geräte fest und ob sie vernetzt sind. Wichtig ist, dass von den anwesenden Personen keine Veränderung mehr am Gerät durchgeführt werden kann. Das ist speziell bei Notebooks heikel. Hier kann es genügen, dass die Person den Deckel schließt und damit ein Verschlüsselungsprogramm aktiviert. Dann sind die Daten auf dem Gerät einfach nicht mehr zu nutzen.
Daher bedarf es hier einer genauen, sorgfältigen Vorbereitung. Denn die Täter sind meist Profis und verwenden Schutzmechanismen. Da reicht oft ein Tastendruck und alle Daten werden gelöscht. Andererseits sind wir auch für die klassische forensische Beweissicherung zuständig, wo es darum geht, Beweise auf Computer sicherzustellen. Dazu werden spezielle Forensik-Programme eingesetzt und international anerkannte best practises angewendet.

kripo.at: Können Sie mit diesen Produkten auch die Daten von Handys auswerten?

Mag. Löschl: Für das Auslesen von Handys haben wir zwei verschiedene Softwareprodukte. Wir verwenden immer verschiedene Software, um auch Geräte unterschiedlicher Marken und Typen auswerten zu können. Nicht jedes Produkt ist für jedes Handy geeignet.

kripo.at: Immer wieder wird behauptet, dass bei der Auslesung von Daten diese verändert werden. Ist dieses Misstrauen berechtigt?

Mag. Löschl: Für uns ist es wichtig, dass Daten nicht verändert werden. Dafür sorgt einerseits das Auswertungsprogramm und zweitens wird ein so genannter Hashwert ermittelt. Das heißt es wird vor der Auswertung der gesicherten Daten ein Wert errechnet der den Datenbestand eindeutig identifiziert. Nach der Auswertung wird dieser Wert neuerlich festgestellt, um zu kontrollieren, ob die beiden Werte auch exakt übereinstimmen. Damit ist garantiert, dass keine Veränderung der Daten vorgenommen wurden. Wir verwenden auch so genannte Schreibblocker, das sind Geräte die verhindern, dass Daten auf den Datenträger zurück geschrieben werden. Die Auswertungen erfolgen dann auf einem Image, die Originaldaten bleiben somit unverändert.

kripo.at: Diese Methode genügt sicher bei Einzelgeräten, aber was machen Sie bei Netzwerken?

Mag. Löschl: Besonders bei Firmen wäre es unverhältnismäßig, wenn man einzelne Geräte abbauen würde, weil dadurch der Geschäftsbetrieb gestört werden könnte und große Schäden entstehen würden. In diesem Fall wird in

der Firma ein Image erstellt oder sofern vorhanden das backup gesichert. Wenn kein backup verfügbar ist oder die Daten veraltet sind, gibt es die Variante, dass man die Daten selektiv kopiert. Gemeinsam mit dem Administrator werden dann bestimmte Bereiche des Netzwerkes kopiert.

kripo.at: Also für derartig hoch spezialisierte Tätigkeit bedarf es doch einer entsprechenden Ausbildung. Welche Ausbildung haben die Beamten in Ihrem Büro?

Mag. Löschl: Unsere Beamten haben eine Spezialausbildung im Bereich Betriebssysteme, Software und forensischer Programme. Das trifft auch auf die Beamten des AB 06 in den Landeskriminalämtern zu. Die Fortbildung erfolgt laufend im Rahmen des KDFR. Im Bundeskriminalamt haben wir auch internationale Fortbildungsveranstaltungen und sind an internationalen Projekten beteiligt, wie zum Beispiel ECTEG (European Cypercrime Training and Education Group). Unsere Beamten nehmen regelmäßig an Schulungen bei ECTEG und bei Interpol, aber auch bei anderen Instituten teil, um aktuelles internationales Knowhow nach Österreich zu bringen. Wichtig sind aber auch die internationale Vernetzung und der Erfahrungsaustausch dieser Beamten. Internationale Kontakte bringen den Vorteil bei gemeinsamen Ermittlungen sofort einen kompetenten Ansprechpartner im Ausland zu haben.

kripo.at: Ihre Beamten haben sicher eine hervorragende Ausbildung, doch wie steht es um das Wissen des „Beamten auf der Straße“?

Mag. Löschl: Computerdelikte und Cybercrime werden bereits im Rahmen der Grundausbildung gelehrt. Wir würden uns natürlich gern noch mehr wünschen und sind hier auch mit der SIAK in Gesprächen. Im Zuge der Kriminaldienstmodule sind die Themen schon ausführlicher behandelt. Diese Schulungen werden von den Beamten des AB 06 durchgeführt. Im Rahmen der Umsetzung unserer Gesamtstrategie Cybercrime ist es zudem vorgesehen, dass in jedem Bezirk mehrere Beamte arbeiten, die spezialisierter ausgebildet sind. Die ersten Beamten wurden bereits im Juni dieses Jahres geschult. Diese Schulung durch das .BK dauert eine Woche, danach erfolgt eine weiterführende Ausbildung mit dem Schwerpunkt Technik im LKA. Die Beamten haben damit eine theoretische und eine praktische Schulung und sollen auch mit entsprechenden technischen Geräten versorgt werden. Sie sind in erster Linie Ansprechstelle für die Beamten vor Ort, fungieren als Schnittstelle in die LKAs und in das .BK und führen auch selbstständig einfache Sicherungsmaßnahmen durch.

kripo.at: Gibt es eigentlich einen typischen Computerkriminellen?

Mag. Löschl: Der Österreichischen Kriminalstatistik zufolge kann man diese Frage nur mit „Nein“ beantworten. Ein Viertel der Täter sind jedenfalls unter 25 Jahre. Je „technischer“ das Delikt, umso jünger die Täter. Zuletzt hatten wir einen Täter mit 15 Jahren, der verschiedene Firmen gehackt hat und über Spielplattformen in die Community und schlussendlich in den kriminellen Bereich abgekommen ist.

kripo.at: Kann man heute schon sagen in welche Richtung sich die Computerkriminalität entwickeln wird?

Mag. Löschl: Durch das Wachstum der Bevölkerung in den Entwicklungsländern können wir davon ausgehen, dass sich das Potential der Täter in diesen Ländern auch rasant vergrößern wird. Dieses Faktum wird sich auf die Computerkriminalität in den Industriestaaten, wie die USA oder Europa und natürlich auch Österreich, auswirken. Die Computerkriminalität wird steigen, auch aufgrund der Tatsache, dass es einfach mehr Zugänge zum Internet geben wird. Weiters wird sich die Cloud-Thematik massiv durchsetzen, auch im privaten Bereich. Der PC zu Hause ist gut, aber heute wollen die Menschen immer und überall Zugang zu ihren Daten haben, das ist mit Smartphones und Tabletts möglich. Ich würde mich nicht als großen Hellseher bezeichnen, wenn ich behaupte, dass die IT-Kriminalität zunehmen wird. Wir haben bereits darauf reagiert und ein Referat „Mobile Forensik“ gegründet, um auch diesen Bereich abdecken zu können.

kripo.at: Wie es scheint, ist der Zustand Ihres Büros zufriedenstellend. Haben Sie keine Wünsche?

Mag. Löschl: Eigentlich wünsche ich mir weibliche Cybercops (lacht). Unsere Sparte ist nämlich eine reine Männerdomäne. Darüber hinaus liegt mir natürlich die rasche Umsetzung der Gesamtstrategie Cybercrime mit dem Cybercrime Competence Center (C4) am Herzen.

• Mit Mag. Leopold Löschl sprachen Helmut Bärtl und Richard Benda

Cybercrime Competence Center (C4)

Im Mai 2011, im Zuge des Sicherheitskongresses des KSÖ, verkündete die neu ins Innenministerium eingezogene Ministerin Johanna Mikl-Leitner, dass eine spezielle Truppe, die gegen Kriminelle einsetzbar ist, die Datenträger und/oder das Internet für ihre Straftaten benützen, geplant sei. Die rasante Steigerung der Internetkriminalität, so die Ministerin, und der notwendige Kampf gegen die Organisierte Kriminalität hätten eine zentrale, nationale Koordinierungs- und Meldestelle notwendig gemacht. Diese Truppe, die im Bereich des .BK angesiedelt ist, erhielt wie bereits in anderen Ländern den Namen Cybercrime Competence Center (kurz C4). C4 soll neben ihrer forensischen Tätigkeit auch als Supportstelle für die Landeskriminalämter dienen und rund um die Uhr zur Verfügung stehen, wenn es Fragen aus dem Bereich Cybercrime, vor allem in technischer Hinsicht, geht. Das C4, so sieht es das Konzept vor, soll weiters als Schnittstelle zwischen Polizei, Wirtschaft, Wissenschaft und Forschung fungieren.

Cyber-Risikoland-schaft Österreich

Die Sicherheit im Cyberraum kann nicht alleine Anliegen des Innenministeriums sein, sondern ist Aufgabe der Sicherheitsbehörden, der Wirtschaft und eigentlich von jedem, der sich auf diesem Gebiet bewegt. Auch Organisationen, allen voran das „Kuratorium Sicheres Österreich (KSÖ)*“ hat dies erkannt und deshalb die „Initiative Cybersecurity“ ins Leben gerufen.

Ende 2012 will die Bundesregierung eine nationale Cybersicherheitsstrategie vorbereiten. So etwas kann nicht aus dem Ärmel geschüttelt werden. Das KSÖ will zu dieser Strategie ihren Beitrag leisten und hat deshalb Cybersecurity als eine der Kernaufgaben seiner Tätigkeit erkoren. Der Ausbau von Know-how und die Sensibilisierung von Behörden und Wirtschaft, der Aufbau eines Expertennetzwerkes und noch viele weitere Ziele abzustecken, war die erste Station. Es folgte im September 2011 eine Risikoanalyse bzw. die Erstellung einer Cyber-Risikomatrix, der wieder Planspiele mit Fokus auf verschiedene Bereiche kritischer Infrastruktur folgten. Ein Zwischenergebnis wurde im Juni dieses Jahres anlässlich des KSÖ-Sicherheitskongresses der fachkundigen Öffentlichkeit präsentiert. Der Kongress, der unter großer internationaler Beteiligung stattfand, diente aber nicht alleine der Bilanzierung, sondern es wurden auch in acht Spezial-Workshops Themen angesprochen und diskutiert.

Ein weiterer, ungewöhnlicher Schritt ist eine „Cybersecurity Challenge“. Seit 28. Juni d.J. wird in einer Art Bewerb eine Talentsuche nach begabten und qualifizierten IKT-Spezialisten in Österreich veranstaltet. Jedes Monat wird in einem virtuellen „Hacking-Labor“ ein Cyber-Rätsel veröffentlicht, das die IT-Talente lösen müssen (www.verbotengut.at) . Auf diese Art sucht man junge Menschen, die das Zeug zum Hacker hätten. Statt illegal und kriminell zu werden, können hier Talente auf die richtige Bahn gebracht werden. Immerhin haben sich bisher rund 300 Bewerber gemeldet. Das Finale des Bewerbes wird am 6. und 7. November über die Bühne gehen.

Vorläufig letztes Kapitel im Kampf gegen die Cyberkriminalität ist ein in Buchform veröffentlichter Bericht über die Situation und Risiken in Österreich. Laut dieser Risikopotenzialanalyse (sie will ausdrücklich nicht als Bedrohungsanalyse verstanden werden) sind die gefährdetsten Bereiche der Energie-, Transport und der Finanzsektor. Eingegangen wird auch auf die Rolle des Menschen selbst im Umgang mit Computer und Internet. Auch der Behördensektor, darüber waren sich die Experten einig, ist verwundbar. Die Bewertung der Risikofaktoren Social Engineering, Cybercrime und Cyberspionage in Verbindung mit der Gefahr des Diebstahls bzw. der Manipulation digitaler Identitäten und Bürgerdaten, wird als hoch eingeschätzt.

Den Abschluss des 122 Seiten starken Berichtes/Buches bilden die Handlungserfordernisse die von Experten vorgeschlagen wurden und ein Glossar, das in einer Art Übersetzung die Begriffe erklärt.

Wer Näheres erfahren will, findet auf der Website des KSÖ (www.kuratorium-sicheres-oesterreich.at) weitere Informationen.

* Die Vereinigung Kriminaldienst Österreich (VKÖ) ist als einzige polizeinahe Organisation Mitglied beim Kuratorium Sicheres Österreich

Erste Waffe aus 3D-Drucker abgefeuert

Ein US-Waffenliebhaber hat aus einer Pistole des Kalibers 22, die zum Teil aus mittels 3D-Drucker hergestellten Plastik-Teilen besteht, 200 Schüsse abgefeuert, wie der New Scientist berichtet. Bei der Waffe handelt es sich um eine Eigenkonstruktion. Aus dem Drucker kommt das untere Gehäuse der Pistole, das mithilfe eines 3D-Modells für eine Komponente des Maschinengewehrs M16 erstellt wurde. Die restlichen Teile sind aus Metall. Laut US-Gesetz ist das Gehäuse der Bauteil, der eine Waffe ausmacht. Hier sitzt auch die Seriennummer, auf der die Waffenkontrolle beruht.

Zum Herstellen der Pistole verwendete der Waffenbauer, der sich im einschlägigen AR-15-Forum HaveBlue nennt, einen Stratasys-Drucker. Die Kosten für die Herstellung des Gehäuses beliefen sich so auf etwa 30 Dollar. Mit günstigeren Geräten könnten der finanzielle Aufwand vermutlich auf zehn Dollar pro Stück gesenkt werden. Die Pläne für das Gehäuse hat HaveBlue veröffentlicht. Ein Plan zur Herstellung eines Sturmgewehrs mit dem Gehäuse ist vorerst gescheitert, weil es Probleme mit den Originalteilen gab.

Tor zu Missbrauch aufgestoßen

Durch die Herstellung eines Gehäuses, das nicht der staatlichen Kontrolle unterliegt, ist das Tor zu Missbrauch von 3D-Druckern in den USA weit aufgestoßen. Reguliert werden nämlich nur die Gehäuse, andere Waffenteile sind auch für Menschen ohne Waffenschein oder solche, denen er entzogen wurde, frei erhältlich.

"Wie bei vielen anderen Technologien besteht auch beim 3D-Druck die Möglichkeit zum Missbrauch. Der Druck von Waffen und anderen potenziell gefährlichen Produkten ist im Zweifelsfall schwierig zu unterbinden, da die Technologie schnell und unkompliziert fast jedes vorstellbare Produkt erzeugen kann. Hier ist die Politik gefordert, eine Lösung zu finden.

Revolution aus dem Drucker

Nicht alles ist negativ. Die positiven Aspekte des 3D-Drucks überwiegen. So könnten aus alten Rohstoffen relativ einfach neue Produkte hergestellt werden. Für den Umweltschutz sicher ein ungeheurer Fortschritt.

Durch 3D-Druck werden aber auch viele andere Bereiche des menschlichen Lebens revolutioniert. Auch die Wirtschaft steht vor einem Umbruch, wenn nur noch gedruckt wird, was auch tatsächlich gebraucht wird. Viele Produkte werden schlicht und einfach nicht mehr im Einzelhandel gekauft werden. Obwohl es noch einige Jahre dauern wird, scheint hier ein bedeutsamer Durchbruch für die Technologie gelungen zu sein.

So wird von Ersatzteilen für die Waschmaschine bis zum Geschirr alles individuell herstellbar sein.

Erste Anzeichen für einen Siegeszug der Technologie gibt es schon. Es existieren schon verschiedene Bereiche, in denen 3D-Druck für den Endkunden bedeutsam ist. Interessant wird diese Technik allerdings auch für Kriminelle verschiedener Provenienz. Daher ist es aber auch absolut wichtig, sich möglichst rasch und umfassend mit allen Gefahren, welche aus dieser Technologie resultieren, auseinanderzusetzen.

• Josef Walter Lohmann

3D-Drucker: Waffenschmiede der Zukunft?

Johann Veith: Magister of Arts

Obwohl schon einige Jahre in Pension, ist „Hans“ Veith in Kriminalistenkreisen noch immer ein Begriff. Seine überquellende Aktivität hat ihn auch in der Pension nicht verlassen und so inskribierte er an der Donau-Universität in das neue Studium „Menschenrechte/ Human rights“. Es gelang ihm als erster und mit Auszeichnung dieses Studium abzuschließen. Er darf seinem Namen nun mit dem Titel „Master of Arts M.A.“ versehen. Wir gratulieren unserem Mitglied.

Döblinger Hauptstraße in neuem Glanz

Die VKÖ ist, wie vermutlich bekannt, Eigentümer der Liegenschaft 1190 Wien, Döblinger Hauptstraße 57. Das Jugendstil-Gebäude ist zwar nicht denkmalgeschützt, doch in dem Ensemble der Gegend ein optischer Anziehungspunkt. Leider erlitt die Fassade in den 70er Jahren einen verhängnisvollen Eingriff, bei einem der Geschäfte wurde das historische Portal entfernt und durch ein Blechportal ersetzt. Im Zuge einer Sanierung des Gebäudes wurde nun auch das ehemalige, historische Portal rekonstruiert, womit die gesamte Fassade wieder dem Aussehen entspricht, die sie bei der Erbauung hatte.

So werden Menschen betrogen

Niemand ist davor gefeit, Opfer eines Verbrechens zu werden. Vor allem ältere Menschen sind dieser Gefahr in erhöhtem Ausmaß ausgesetzt, vor allem durch Betrüger. Obwohl die meisten Tricks von Betrügern bekannt sind und schon Jahrzehnte eingesetzt werden, fallen immer wieder Menschen darauf herein.
Die VKÖ hat sich des Themas angenommen und seit Anfang Oktober liegt die Broschüre „Mit List und Tücke – so arbeiten Kriminelle“ zur Verteilung auf – gratis natürlich. Neben der Broschüre wird als zweite Schiene eine Veranstaltungsreihe mit dem gleichen Thema durchgeführt. Die erste Veranstaltung findet am
25. Oktober 2012, um 19.00 Uhr in der Volkshochschule Liesing, 1230 Wien, Perchtoldsdorferstraße 3/großer Saal statt. Selbstverständlich ist der Eintritt frei. Im Anschluss stehen Beamte des kriminalpolizeilichen Beratungsdienstes für individuelle Fragen zur Verfügung.

Tatwerkzeug Computer: Erster Angriff an einem Tatort

Der Verband Europäischer Gutachter und Sachverständiger (VEGS)bietet zu dem Thema „Erster Angriff an einem Tatort“ eine eintägige Schulung für Polizeibeamte an. Bei der Schulung werden die grundsätzlichen Verfahrensweisen gelehrt, um bei Sicherstellung von Computern oder anderer technischen Geräte keine Spuren zu vernichten, so dass diese für eine spätere Auswertung von Fachpersonal unbeschädigt zur Verfügung stehen. Auf Grund der Komplexität des Wissens wird die Schulung nur für Kleingruppen (6 – 10 Personen) angeboten. Die Kosten einer Teilnahme betragen pro Person Euro 275,-.
Die VKÖ würde bei Interesse einen Kurs in Wien durchführen. Mitglieder würden den üblichen Bildungszuschuss von Euro 100,- erhalten.
Interessenten können sich per mail sekretariat@kripo.at oder telefonisch unter 050 133 133 bei uns melden.

IMPRESSUM
Eigentümer und Herausgeber: Vereinigung Kriminaldienst Österreich
A-1090 Wien, Müllnergasse 4/8, Tel. 050133133
E-Mail: redaktion@kripo.at
Präsident: Richard Benda
Chefredakteur: Prof. Josef W. Lohmann
Redaktionssekretariat: Birgit Eder
Gestaltung: Christian Doneis
Mitarbeiter: Richard Benda, Prof. Josef W. Lohmann, Tam Hanna, Ludwig Hinterkörner, Willibald Plenk, Herbert Zwickl, Mag. Manfred Zirnsack, Mag. Max Edelbacher, Helmut Bärtl, Peter Grolig, Frank Dieter Stolt

Redaktionsadresse:
Redaktion der **kripo.at**, A-1090 Wien, Müllnergasse 4/8, E-Mail: redaktion@kripo.at
Der Nachdruck von Artikeln ist nur nach Absprache mit der Redaktion mit Quellenangabe zulässig.
Sektionsleiter in den Bundesländern:
Steiermark: Graz, Paulustorgasse 8, 059 133 60, Karl Strohmeier
Tirol: Innsbruck, Kaiserjägerstr. 8, 059 133 70, Wolfgang Knöpfler,
Kärntnen: Klagenfurt, St. Ruprechterstraße 3, 059 133 253101, Harald Jannach,
Oberösterreich: Linz, Nietzschestraße 33, 059 133 45-7526, Helmut Kaiser,
Wels, Dragonerstraße 29, 059 133 4190-324, Martin Müllner,
Steyr, Berggasse 2, 059 133-4140 324, Josef Fuchshuber
Niederösterreich: St. Pölten, Linzer Straße 47, 059 133 35-3311, Werner Steinböck,
Salzburg: Salzburg, Alpenstraße 1, 059 133 55-3404, Johann Bründlinger

Verleger: Informations- u. Verlagsgesellschaft m.b.H., A-8073 Feldkirchen b. Graz, Thalerhofstraße 28. **Anzeigenverwaltung:** A-8073 Feldkirchen b. Graz, Thalerhofstraße 28 **Hersteller:** DHT Feldkirchen b. Graz, Gmeinergasse 1-3. **Verlags- und Herstellungsort:** A-8073 Feldkirchen b. Graz **Verlagspostamt:** A-8073 Feldkirchen. Der Nachdruck von Inseraten, die in diesem Heft erscheinen, ist nur mit ausdrücklicher Genehmigung des Verlegers gestattet. Bei von Angehörigen des öffentlichen Dienstes verfassten Beiträgen handelt es sich um deren persönliche Ansicht als Privatperson und nicht um jene der Behörde.

Offenlegung gemäß § 25 Mediengesetz:
Medieninhaber: Informations- u. Verlagsgesellschaft m.b.H.
Grundlegende Richtung: **„kripo.at“** ist ein Informationsmedium für Exekutivbeamte und die an Sicherheitsfragen interessierten Bürger. DVR-Zahl: DVR 08885606
„kripo.at“ erscheint sechsmal jährlich, wird allen Mitgliedern kostenlos zugesandt und ist nur per Postzustellung zu beziehen. ***www.kripo.at***
Veröffentlichung nach Pressegesetz.

Unsere Kooperationspartner

WIENER UND LINZER MITGLIEDER-TREFFS

„MITGLIEDERTREFF DER WIENER“

Jeden 1. Montag im Monat
ab 17.00 Uhr
Gasthaus „d‘Landsknecht“
Porzellangasse/Ecke Thurngasse,
1090 Wien

„MITGLIEDERTREFF DER LINZER“

Jeden 1. Dienstag im Monat ab 15.00 Uhr
Polizei-Sportbuffet,
Linz, Derflingerstraße Nr. 5

"KRIPO STAMMTISCH WELS"

jeden 1. Dienstag im Monat
ab 16.00 Uhr im PSV Heim

TODESFÄLLE

Karl WETZLMAIER,
Salzburg
im 88. Lebensjahr

Heinrich WIMMER
Linz
im 81. Lebensjahr,

kripo.at TERMINE

Einladung:
Vollversammlung 2012

Datum:

Freitag, 9. November 2012, 18.00 Uhr

Ort:

Hotel Regina, 1090 Wien, Rooseveltplatz 15
(hinter Votivkirche)

Tagesordnung:

1) Begrüßung und Feststellung der Beschlussfähigkeit
2) Vertagung auf 18.30 Uhr sofern notwendige Teilnehmerzahl nicht erreicht wird
3) Neuerliche Begrüßung
4) Bericht des Präsidenten
5) Berichte der Vorstandsmitglieder
6) Bericht der Rechnungsprüfer
7) Entlastung des Vorstandes
8) Berichte der Sektionsleiter
9) Ehrungen
10) Anträge
11) Vorschau auf 2013 und Schlussworte

Zutritt zur Vollversammlung haben nur Mitglieder und geladene Gäste. Anträge sind bis 5. November 2012 in schriftlicher Form dem Sekretariat zu übermitteln.
Zur Vereinfachung der Zutrittskontrolle wird empfohlen beim Eingang den Mitgliedsausweis vorzuweisen.

Ab 17.30 Uhr findet eine Weinverkostung statt.

kripo.at thema

Betrüger arbeiten mit List und Tücke

Die Facetten der Kriminalität sind vielfältig. In den Medien herrscht der Eindruck vor, als ob es nur Mord und Suchtgiftdelikte geben würde. Das Publikum lechzt nach Blut, aber es erzeugt damit eine falsche Gewichtung.

Kriminalität beginnt bei Delikten, die kaum die unsichtbare Linie zwischen straffrei und strafbar überschritten haben, gemeinhin werden sie als Bagatelldelikte bezeichnet. Die Kriminalstatistik spricht hier eindeutige Zahlen. 535.000 Straftaten sind 2010 in der polizeilichen Kriminalstatistik ausgewiesen. Während in der Deliktgruppe Leib und Leben, das sind jene Delikte über die die Medien gerne berichten, 85.000 Straftaten aufscheinen, sind jene des kriminellen Vermögenstransfers, also Delikte gegen fremdes Vermögen, mit 421.000 Straftaten vertreten. Man kann es auch anderes ausdrücken: Die Chance in Österreich körperlich angegriffen zu werden ist verschwindend gering, während jene, Opfer von Diebstahl oder Betrug zu werden, 5-mal so hoch ist.

Öffentliche Wahrnehmung stimmt nicht.

Selbst bei den Delikten gegen fremdes Vermögen stimmt die öffentliche Wahrnehmung nicht. Immer wieder hört man, dass da und dort eingebrochen wurde, dass dieses oder jenes Auto gestohlen oder aufgebrochen worden ist. Doch wie oft hört man, dass jemand durch einen Betrug abgezockt worden ist? Kaum. Der Grund liegt unter anderem darin, dass die Opferrolle bei einem Einbruch oder einem Diebstahl völlig klar ist. Hier ist der Täter – dort das unbeaufsichtigte Auto oder die leere Wohnung. Es besteht kein Kontakt, also kann es auch keinen Fehler von Seite des Opfers geben. Mitleid der Umgebung ist so gesichert.

Anders beim Betrug, nicht selten werden die Rollen vertauscht. Das Opfer wird in die Rolle der Mitschuld gedrängt. Wer Opfer eines Betrügers wird, der ist irgendwie selbst an seinem Unglück Schuld, so die klassische Meinung innerhalb der Bevölkerung. Immer besteht beim Betrug ein Kontakt zwischen Täter und Opfer und sei dieser auch nur via Internet oder Telefon. Das Opfer erkennt auch im Nachhinein in vielen Fällen seine Fahrlässigkeit oder schlicht seine Dummheit und schämt sich seines Verhaltens. Da bei vielen Betrugsfällen die Schadensumme auch klein ist, wird keine Anzeige erstattet. Selber Schuld denkt das Opfer hätte ich nicht…….! Die Polizei weiß oft nichts von Betrügern die ein ganzes Gebiet abgrasen, so geht der Betrug an der Öffentlichkeit vorbei. Nur wenn die Betrüger zu dreist werden und fast epidemieartig mit dem s.g. Neffentrick alte Damen abzocken, dringt hie und da etwas an die Öffentlichkeit.

Broschüre mit Tipps und Hinweisen

Unerkannt bleiben auch viele einfache Diebstähle. Nicht selten glaubt das Opfer seine Geldbörse oder einen anderen Wertgegenstand verloren zu haben, dabei wurde es gestohlen. Auch hier ist die Anzeigehäufigkeit mehr als gering. Wegen einer Geldbörse mit 50 Euro geht heute niemand mehr zur Polizei. Schade, denn auch im Bereich des Taschendiebstahles ist die Dunkelziffer dadurch sehr hoch.

Der Vereinigung Kriminaldienst Österreich ist die Problematik nicht unbekannt, schließlich arbeiten unsere Mitglieder auf diesem Gebiet. Wir haben uns daher entschlossen eine Broschüre zu veröffentlichen, die mit Tipps und Hinweisen, präventiv wirken soll. Zu glauben, man sei der Massenkriminalität, den s.g. Bagatelldelikten, hilflos ausgeliefert, ist falsch. Nachdenken, wachsam sein, nicht auf jedes scheinbar lukrative Geschäft einsteigen ist die erste Verteidigungslinie. Diese Vorbeugungsmaßnahmen sollten immer und überall gelten. Sich über die Arbeitsweise von Kriminellen zu informieren, ist die zweite Linie.

Im Lauf der nächsten Monate wird die Broschüre „Mit List und Tücke – so arbeiten Kriminelle“ in ganz Österreich zur Verteilung kommen. Vorexemplare werden den Sektionen noch heuer zugesendet werden.

Begleitend zu der Erscheinung der Broschüre werden in verschiedenen Städten Präventionsveranstaltungen zum Thema durchgeführt, bei denen auch die Broschüren verteilt werden. Entnehmen Sie bitte die Termine unserer Ankündigung in den Folgeausgaben von kripo.at

• Richard Benda,
Präsident VKÖ

Zahlen, Ziffern, Zeichen
Ein ungewöhnlicher Tatort

Mit zunehmender Nutzung sozialer Netzwerke verlagern sich auch Ehr- und Urheberrechtsverletzungen sowie der unlautere Wettbewerb mehr und mehr auf Online-Plattformen. Über die Pflichten der Plattformbetreiber wird weltweit gestritten.

Es mag an der vielleicht zu schlichten Übersetzung aus dem Englischen liegen, aber soziale Netzwerke sind in vielerlei Hinsicht alles andere als das, was man sich gemeinhin unter "sozial" vorstellt. Ehrverletzungen im persönlichen sowie unlauterer Wettbewerb im unternehmerischen Bereich sind - schon aufgrund der mittlerweile massenhaften Nutzung - an der Tagesordnung. Auch Raubkopien von Software, Musik- oder Filmwerken sowie ihre Verbreitung verlagern sich mehr und mehr auf die sozialen Netzwerke, zumal die Möglichkeiten, dort Inhalte einzustellen oder zu verlinken, immer umfangreicher werden.

Das Fatale für die Betroffenen ist, dass die gesetzeswidrigen Veröffentlichungen ohne jegliche redaktionelle Vorabprüfung von jedermann für jedermann von einem Moment auf den nächsten der Weltöffentlichkeit zur Verfügung gestellt werden - ein Effekt, der bereits seit der Verbreitung des Internets besteht, auf den sich unsere Rechtsordnungen aber immer noch nicht hinreichend eingestellt haben.

Anonymität

Im persönlichen Bereich kommen Gesetzesverstöße überproportional dort vor, wo es den Tätern möglich ist, in den Netzwerken anonym zu bleiben. Und das ist zunächst einmal auch ihr gutes Recht, denn die Betreiber von sozialen Netzwerken sind als Diensteanbieter verpflichtet, die Nutzung und Bezahlung ihrer Dienste auch anonym oder unter Pseudonym zu ermöglichen. Nicht zuletzt deshalb hat etwa auch Google bei seinem erst kürzlichgestarteten Netzwerk "GooglePlus" den zunächst etablierten Klarnamenzwang noch im gleichen Jahr wieder abgeschafft. Der Gesetzgeber steht damit zunächst vor dem klassischen Zielkonflikt zwischen berechtigten Interessen des Datenschutzes und den berechtigten Interessen der durch die gesetzeswidrigen Inhalte betroffenen Personen oder Unternehmen. Das wird an folgendem Beispiel deutlich:

Probleme mit Kreditkarten

Ein anonymer Blogger hatte auf einem Internetportal einem Geschäftsmann unterstellt, er habe Rechnungen eines Sexklubs auf Mallorca mit seiner Firmenkreditkarte bezahlt. Der Geschäftsmann wies das als unwahr und ehrenrührig zurück. Weil der Autor des Textes nicht zu ermitteln war, klagte er gegen den Betreiber des Portals als zuständigen Host-Provider wegen Verbreitung ehrenrühriger Tatsachenbehauptungen auf Unterlassung. Verschiedene Instanzen gaben der Klage statt. Der Betreiber des Portals ging in die Revision vor die Höchstinstanz. Diese bestätigte daraufhin im Grundsatz die Urteile aus den Vorinstanzen. Mangels eindeutiger gesetzlicher Regelungen löste der zuständige Senat aber den Zielkonflikt zwischen Daten- und Persönlichkeitsschutz auf, indem er Portalbetreibern und deren Nutzern wechselseitige Pflichten auferlegte.

Zunächst müssen die Provider nur dann tätig werden, wenn der Betroffene auf die Ehrverletzung so konkret hinweist, dass der Provider den Verstoß gegen das Persönlichkeitsrecht auf Grundlage der Behauptungen unschwer, also ohne eingehende rechtliche und tatsächliche Prüfung, nachvollziehen kann. Ist das der Fall, muss der Betreiber des Internetforums oder des sozialen Netzwerks die Beanstandung des Betroffenen an den anonymen Blogger zur Stellungnahme weiterleiten. Äußert sich dieser nicht innerhalb einer angemessenen Frist zu dem Vorwurf oder kann er keine berechtigten Zweifel an der vorgetragenen Ehrverletzung vorbringen, wird vermutet, dass die Beanstandung berechtigt ist. Der Provider muss den betreffenden Eintrag dann löschen. Nimmt der Blogger hingegen substanziiert Stellung und ergeben sich daraus erhebliche Zweifel an dem vorgebrachten Rechtsverstoß, muss der Provider das dem Betroffenen mitteilen und von ihm Nachweise für die behauptete Rechtsverletzung verlangen.

Schadenersatz

Das Urteil bestätigt, dass Opfer von Beleidigungen oder Verleumdungen im Netz gegen rechtswidrige Herabsetzungen vorgehen können. Der Europäische Gerichtshof (EuGH) vertritt eine ähnliche Auffassung. In einem Urteil vom 25. Oktober 2011 haben die Luxemburger Richter entschieden, dass Kläger wegen Persönlichkeitsrechtsverletzungen im Internet ihren gesamten Schaden sogar bei jedem zuständigen EU-Gericht geltend machen können, gleich, wo der Webseitenbetreiber seinen Sitz hat.

Speziell für Betreiber von sozialen Netzwerken folgt aus diesen Urteilen, dass künftig ein klares Prozedere einzuhalten ist. Den Hinweisen von Betroffenen, die sich verleumdet oder beleidigt fühlen, sollte man nachgehen und letztlich entscheiden, inwieweit der Vorwurf ausreichend nachvollziehbar und glaubhaft ist, um die richtigen Schritte zu veranlassen. Das dürfte zwar einen erheblichen Aufwand bedeuten, beseitigt aber auch eine beträchtliche Rechtsunsicherheit auf diesem Gebiet.

Daher entfernen die meisten Betreiber sozialer Netzwerke die auf ihrer Plattform eingestellte Software, Musik- oder Filmwerke

im Falle der Anmeldung entgegenstehender Nutzungsrechte. Das ist insbesondere der zunehmend strengeren Rechtsprechung wegen notwendig. Danach haften die Plattformbetreiber für Inhalte, die von ihren Nutzern eingestellt werden, zwar grundsätzlich nicht, jedoch müssen sie unter Umständen als so genannte Störer tätig werden, wenn sie von rechtswidrigen Inhalten in Kenntnis gesetzt werden. In den USA wurde mit dem Digital Millenium Copyright Act eine entsprechende Notice-and-takedown-Regelung geschaffen.

Kampf gegen Windmühlen

Damit ist aber weder die Frage beantwortet, wie der Betroffene etwaige Schadenersatzansprüche gegen den eigentlichen anonymen Verursacher durchsetzen kann, noch auf welche Weise derartige Gesetzesverstöße präventiv verhindert werden können. Ist eine Verleumdung erst einmal via Facebook verbreitet, nützt es mitunter wenig, den Betreiber der Seite zu verpflichten, die Verleumdung zu entfernen. Ebenso kämpfen Inhaber urheberrechtlich geschützter Nutzungsrechte oft gegen Windmühlen, wenn sie die Veröffentlichung des einen Nutzers aus dem Netzwerk löschen lassen, während ein anderer Nutzer den gleichen Inhalt wieder einstellt.

Prävention

Ungeachtet der Möglichkeiten, die betroffene Personen oder Unternehmen im Nachhinein in Bezug auf den Verletzer oder den Plattformbetreiber haben, stellt sich die Frage, was hinsichtlich einer besseren Prävention geschieht. Weltweit ist eine Diskussion im Gange, ob man den Betreibern sozialer Netzwerke oder anderer Internetplattformen gesetzlich weitergehende Pflichten auferlegen sollte, damit wenigstens die offensichtlich gesetzeswidrigen Inhalte gar nicht erst öffentlich zugänglich gemacht werden.

Diesen in die Jahre gekommenen Verhandlungen tut es gut, dadurch für die "Piratengeneration" geöffnet zu werden, ohne dabei die althergebrachten, aber nicht minder aktuellen Rechte aus dem geistigen Eigentum, der persönlichen Integrität und des fairen Wettbewerbs aus den Augen zu verlieren. Eine Verlagerung von der Ministerebene in die Parlamente sowie in die politischen Parteien ist mit Sicherheit ein besserer Weg als ein Cyberwar via Facebook und Wikipedia.

Den durch Rechtsverstöße betroffenen Mandanten ist bis auf Weiteres zu raten, sich von Rechtsverletzungen nicht einschüchtern zu lassen und im Nachhinein die eigenen Rechte so gut wie möglich wahrzunehmen. Plattformbetreiber sollten in ihrer Budgetplanung zukünftig einkalkulieren, dass die Verbesserung der Prävention zusätzliche Kosten verursachen wird. Und für uns "gewöhnliche" Internetnutzer hilft wie so oft die goldene Regel der praktischen Ethik: "Was du nicht willst, das man dir tu', das füg auch keinem anderen zu" - auch nicht im sozialen Netzwerk.

• Oberst Willibald Plenk

Taliban als attraktive Mädchen

Die australischen Behörden stellen ein großes Sicherheitsrisiko fest und orten einen unverantwortlichen Umgang der Militärs mit Facebook. In dem Bericht steht, dass das Problem "offensichtlich unterschätzt" wird und dass sich die Soldaten "in trügerischer Sicherheit wiegen". Die Behörden warnen ausdrücklich vor gefälschten Profilen und Taliban, die sich als attraktive Mädchen ausgeben, um an Informationen aus erster Hand zu kommen.

Aufständische Taliban greifen immer öfter zu modernen Mitteln, um Terroristen zu rekrutieren und Attacken auf US-Einrichtungen zu provozieren (pressetext berichtete: http://bit.ly/PEfbIt). "Es ist noch zu früh, um von einem Trend zu sprechen. Man kann aber sagen, dass die Taliban, wie der Rest der Welt, auf sozialen Netzwerken präsent sind. Wie effektiv sie tatsächlich sind, können wir noch nicht einschätzen", beschreibt T.G. Taylor von der US-Army http://army.mil die Situation.

Auch Twitter infiltriert

Aber nicht nur Facebook ist ins Visier der Taliban geraten. Auch Twitter wird von den Radikalen zunehmend für PR-Zwecke eingesetzt. Taliban-Sprecher Zabihullah Mujahid sagt, dass man die Nutzung des Internets sofort verbieten würde, wenn es für "antiislamische" Zwecke genutzt würde. Fürs Erste sei man aber damit zufrieden, es für eigene PR-Zwecke einzusetzen.

Die Taliban sind nicht die einzige radikale Organisation, die das Internet für sich entdeckt hat. Wie der Nachrichtensender Al Jazeera berichtet, sind am Sonntag Anhänger der "Syrian Electronic Army" in das Netzwerk des Medienunternehmens eingedrungen und haben gefälschte Nachrichten an die Nutzer versendet. Es wurde das Gerücht verbreitet, dass der Premierminister von Katar einem Attentat entflohen sei.

Die Anfälligkeit der westlichen Streitkräfte hat eine Kritikwelle ausgelöst. Viele Militärs verlangen ein absolutes Verbot von Facebook und Twitter. "Ich beobachte viele Soldaten, die Bilder und Informationen veröffentlichen, die für die Taliban interessant sein könnten", sagte ein Soldat.

Experimentierfeld Polizei:

Von Alpha bis Omega

Wie viele Reformen hat die Polizei schon erlebt, besser vielleicht überlebt? Eine Frage die ad hoc kaum zu beantworten ist, die wir aber vielleicht nach Ende dieser Serie klären können. Ist die erst im September durchgeführte Reform der große Wurf oder nur das vorläufig letzte Glied einer Reformkette?

Die neuen Poizeidirektoren

Die Aussagen der diversen, amtierenden Innenminister zu „ihrer" jeweiligen Reform gleichen sich wie ein Ei dem Anderen: Mehr Effizienz, Einsparungen von Geld und Personal, vor allem aber mehr Beamten auf der Straße. Wenn diese Aussagen tatsächlich stimmen würden, dann müsste unsere Polizei wohl die beste der Welt sein, nichts kosten und kaum Personal haben und vor allem die gesamte Mannschaft müsste auf der Straße sein. Der gelernte Österreicher weiß, dass Politikeraussagen in ihrem Wahrheitsgehalt an Grimms Märchen herankommen. Natürlich bewegen Reformen, natürlich wird da und dort Personal und damit Geld eingespart, doch in der Mehrheit der Fälle wird nur verschoben und Türschilder ausgewechselt. Über das „Mehr Beamte auf der Straße" legen wir überhaupt besser den Mantel des Schweigens. Der von der derzeitigen Innenministerin Mag. Johanna Mikl-Leitner zur Reform 2012 kreierte Slogan: „Näher am Bürger, schneller, effizienter, schlanker" klingt gut, doch erst die Zukunft wird zeigen, ob diese Reform hält, was sie verspricht. Auch die Einsparungen von vorausgesagten acht bis zehn Millionen nehmen wir gerne zur Kenntnis.

Wunsch: Personaleinsparung

Eine Regelmäßigkeit, die sich durch fast sämtliche Reformen der letzten Jahre zieht, ist der Wunsch von Personaleinsparung. Der sinkende Personalstand der Exekutive in Österreich ist genug Beweis dafür, dass diese Vorgabe fast immer die Einzige ist, die tatsächlich greift. Der Haken dabei ist, dass üblicherweise diese Einsparung von unten beginnt und höchst selten die Führungsetagen trifft.

Bei der soeben abgeschlossenen Reform soll das anders sein. Nicht bei den Indianern, sondern bei den Häuptlingen wurden Sesseln entfernt. Für die einzelnen Abteilungen und Polizeiinspektionen soll sich, außer im innerdienstlichen Betrieb, nichts verändern, heißt es.

Aus 31 mach 9

lautet das Motto der Reform 2012. Die Sicherheitsdirektionen, die Bundespolizeidirektionen und die Landespolizeikommanden werden per Gesetz zu einer Behörde zusammengeführt, sie sind damit sowohl Sicherheitsbehörde, als auch und auch Dienstbehörde für den exekutiven Dienst. Die bisherigen Polizeidirektionen in anderen Städten (z.B. Leoben) sind nur mehr Außenstellen und werden in Hinkunft als Polizeikommissariate bezeichnet. Zwar ein Prestigeverlust für manchen Behördenleiter, aber keine existenzielle Bedrohung.

In Wien sind die personellen Veränderungen überhaupt überschaubar, lediglich aus dem Landespolizeikommandanten

Kaum gegründet schon reformiert

Der Grundstein der Kriminalpolizei in Österreich wurde nach der Revolution 1848 gelegt. Vor diesem Zeitpunkt genügten dem Staat polizeiliche Spitzeln, denn eine kriminalpolizeiliche Tätigkeit in unserem heutigen Sinn gab es nicht. Für die „Obrigkeit" stand vorwiegend die politische und religiöse Gesinnung der Bürger im Zentrum des Interesses und nicht die Aufklärung von Straftaten.

Die Veränderung des Revolutionsjahres führten 1850 zur Errichtung von Polizeidirektionen und Kommissariaten, womit endlich die Polizei von der militärischen Gewalt getrennt wurde. Für die Polizei als ziviler Wachkörper war der 20.4.1852 von Bedeutung, es wurde eine Instruktion für die „Zivilwachgemeinen" erlassen und damit endlich das Spitzelsystem metternichscher-sed-Initzkyscher Prägung abgelöst. Die neue Art der Polizei sollte sich „auf die stille, unauffällige Beobachtung und die Anzeige des Wahrgenommenen beschränken". Wobei unter „Zivilwachgemeinen" nicht in Zivil tätige Beamten gemeint waren, sondern lediglich nicht militärische.

Die rechtliche Stellung dieser polizeilichen Urahnen war mehr als triste. Es gab keine Pension und die Beförderung erfolgte „nach Verdienstlichkeit". Die Beamten waren dauernd im Dienst und über die dienstfreie Zeit entschied der Vorgesetzte. Diese Truppe von schlecht bezahlten und abhängigen armen Teufeln war natürlich nicht imstande, die am Beginn des Industriezeitalters emporwachsende Kriminalität zu

Die Beamten hoffen, dass nach dieser Reform endlich Ruhe einkehrt.

Karl Mahrer, wird nun ein Landespolizeivizepräsident. Auch bei den einzelnen Leitern der Abteilungen gibt es weder organisatorisch, noch personell Überraschungen. Kleine Änderungen in der Wertigkeit, wie z.B. die Aufwertung des Polizeiärztlichen Dienstes, sind nett, gehen aber nicht wirklich an die Substanz.

Die Stellvertreter des Landespolizeipräsidenten bekommen jeweils einen bestimmten Arbeitsbereich zugewiesen. Der Geschäftsbereich A (in Wien Karl Mahrer) übernimmt die Aufgaben Strategie und Einsatz. Geschäftsbereich B (in Wien Dr. Michaela Kardeis) ist künftig für Verfahren und Support zuständig. Diesem Triumvirat nachgeordnet sind die einzelnen Fachabteilungen, bei der Kriminalpolizei sind das das Landeskriminalamt und das Landesamt für Verfassungsschutz. Zum Leiter des LKA Wien und damit zum obersten Kripo-Beamten wurde Brigadier Josef Kerbl bestellt. Als Leiter des LV-Wien wurde Hofrat Mag. Erich Zwettler eingesetzt.

Wie weit sich die Änderung der bisherig horizontalen Gliederung auf eine vertikale auf den Dienst an der Front auswirken wird, kann man jetzt noch nicht beurteilen. Der eklatante Personal- und Ausstattungsmangel in Wien, den die Personalvertreter ankreiden, wird jedenfalls durch diese Reform nicht gebessert.

Verunsicherung

Also wieder eine Reform die nichts bringt außer Verunsicherung? Nun, nicht ganz. Die Polizei in den Bundesländern trifft die Reform schon mehr. Nehmen wir als Beispiel Oberösterreich. Verständlich, wenn die Strategen im Innenministerium sagen, dass es nicht notwendig sei drei Polizeidirektionen (Linz, Wels, Steyr) plus eine Sicherheitsdirektion innerhalb eines Radius von 100 km zu haben. Also, Angleichung der Struktur an die anderen Bundesländern und nur ein Polizeidirektor für Oberösterreich. Wenn man bei der Kripo noch dazurechnet, dass es auch das Landeskriminalamt gibt, dann kommt man in diesem Bundesland auf die Formel: Aus 5 mach 1. Hier kann man tatsächlich von einer Verschlankung der Organisation sprechen, denn fünf Abteilungen die mehr oder weniger dasselbe Feld beackern, bedürfen einer Menge von Schnittstellen. Auch für die Gerichte und Staatsanwaltschaft hat diese Reform einen Vorteil, sie müssen nunmehr nur mit einer Stelle kommunizieren.

Die Mehrheit der Beamten hofft jedenfalls, dass mit dieser Reform endlich Ruhe einkehrt und eine Zeit lang von weiteren Reformen Abstand genommen wird.

• Richard Benda

Ein Organigramm der Sicherheitsbehörden in Österreich und der Landespolizeidirektion Wien, sowie ein Verzeichnis der Namen der Abteilungsleiter finden Sie auf unserer Homepage:
www.kripo.at/news

bekämpfen. Um eine Zentralisierung der kriminalpolizeilich tätigen Beamten zu erreichen, wurde am 11.1.1858 eine „Normale“ erlassen, dass die Gründung eines „Büros für öffentliche Sicherheit“ gestattete. So gesehen erfolgte schon die Gründung der Kriminalpolizei durch eine Reform, aber war es auch der Geburtstag? Als möglichen Geburtstag könnte man eher den 25.12.1870 bezeichnen. An diesem Tag wurde das k.u.k. Polizeiagentkorps gegründet, dass aber erst am 1.3.1872 tatsächlich ins Leben gerufen wurde. Die Eigenständigkeit der Kripo führte zu einer Blüte, unter anderem auch weil erstmalig Aufnahmebedingungen und Prüfungen zum Eintritt in das Korps vorgeschrieben waren. Diese erste Blüte war natürlich auch durch die parallel laufende Entwicklung der Kriminalistischen Wissenschaften bedingt.

Reform Nummer 1 erfolgte schon wenige Jahre nach der Gründung. Bis 1875 waren alle Wiener k.u.k. Agenten auf das Sicherheitsbüro konzentriert, während in den Bezirken uniformierte Beamte ihren Dienst versahen. Vorerst versuchsweise wurden in diesem Jahr 50 Polizeiagenten auf die verschiedenen Kommissariate versetzt, um dort ausschließlich „Indagationsdienst“ zu versehen. Die Entwicklung bewährte sich und 1890 waren bereits 26 Inspektoren und 348 Polizeiagenten diszlogiert tätig. 1914 wurde ein einheitliches Dienstrecht geschaffen. Die kriminalistischen Wissenschaften hatten zwischenzeitlich bedeutende Fortschritte gemacht und das Fachpersonal dafür rekrutierte man aus dem Agentkorps. Keine Reform im eigentliche Sinn, aber eine wesentliche Ausweitung des Tätigkeitsbereiches.

Einen abrupten Abbruch in der Entwicklung der kriminalpolizeilichen Arbeit bedingte der 1. Weltkrieg. Die Kripo wurde zwar nicht grundsätzlich reformiert, doch ihre Arbeit veränderte sich neuerlich. Die Agenten wurden für die Zensur und zur Unterstützung der Militärbehörden bei der Spionageabwehr eingesetzt, ein Niedergang der Wiener Kriminalistischen Schule war die Folge. Das Ende des Weltkrieges war für die Polizeiagenten mehrfach erfreulich. Nach Ende des Krieges konnten sie wieder in ihrem eigenen Bereich arbeiten und mit 30.10.1919 wurde ihnen die Beamteneigenschaft zugesprochen. Als Weihnachtsgeschenk in diesem Jahr, am 24.12.1919, gab es eine wesentliche Reform, aber darüber lesen Sie mehr in unserer nächsten Ausgabe.

Spektakuläre Kriminalfälle

Im Rahmen der Ausstellung “Geschichte des Grauen Hauses” befassten sich zwei Vorträge mit dem Themenkreis: “Spektakuläre Kriminalfälle”. Am 4. September 2012 durfte ich im Großen Schwurgerichtssaal vor etwa 250 Besuchern sprechen.

Es war ein beeindruckendes Gefühl einmal an der Richterbank auf dem Stuhl des Vorsitzenden sitzen zu dürfen. Als Polizist wurde man ja fallweise als Zeuge geladen und stand dann vor dem Richtertisch, um Stellung zu nehmen. Der Große Schwurgerichtssaal im Grauen Haus beeindruckt allein schon durch seine Dimensionen.

Ich berichtete über die Geschichte des Sicherheitsbüros und meine berufliche Zeit als letzter Vorstand dieser Einrichtung. Einen ganz entscheidenden Beitrag zur inhaltlichen Gestaltung der Arbeit von Polizei- und Justiz lieferte der Grazer Kriminologe Univ. Prof. Dr. Hans Groß. DDr. Christian Bachhiesl schrieb in seinem Buch „Der Fall Josef Streck“: „In Graz hatte sich neben dem Strafrecht eine weitere Wissenschaft etablieren können, die sich mit dem Verbrechen und den Verbrechern auseinandersetzte: die Kriminologie. Nach lange Jahre währenden Ringen um die Erhöhung der Kriminologie zu einer eigenständigen Wissenschaft war es Hans Groß (1847-1915), dem nachmals für seine Verdienste als „Vater der Kriminologie“ betitelten Juristen und zähen Bekämpfer aller nur denkbaren Formen des Verbrechens, gelungen, ein eigenes Institut für Kriminologie an der Grazer Universität zu etablieren und diesen Forschungsbereich von seinem Status als bloße Hilfswissenschaft des Strafrechts zu befreien. Hans Groß leitete das Institut für Kriminologie bis zu seinem Tode im Jahr 1915. Mit seinem „Handbuch für Untersuchungsrichter, Polizeibeamte, Gendarmen …“, Graz 1894, schuf er Standards der Tätigkeit von Justiz und Polizei, die bis heute Gültigkeit haben.

Die sieben Goldenen „W“

Die sieben Goldenen „W“ der Fragetechnik bilden die unverzichtbare Grundregel jedes Verhörs (Was, Wann, Wo, Wie, Womit geschah von Wem und Warum).

Auf diesen theoretischen und praktischen Grundlagen der Grazer Schule der Kriminalistik schuf die Wiener Schule der Kriminalistik im Zusammenwirken mit der Wiener Schule der Gerichtsmedizin eine wesentliche Qualitätsverbesserung der kriminalistischen Arbeit. Da in der Gründerzeit der Zuzug nach Wien sehr stark anstieg, verschlechterten sich die sozialen Lebensbedingungen der Menschen und auch die Kriminalität nahm zu. Dieser Nährboden für Gewaltdelikte führte zu einer Verbesserung der Kriminaltechnik, einer engen Kooperation mit der Wiener Gerichtsmedizin und zu einer Blüte der

Der Klimtsaal

Präsident und Gastgeber Mag. Forsthuber war sichtlich beeindruckt

Wiener Schule der Kriminalistik. Die Wiener Polizei erlangte ein derart hohes Niveau, dass sie anfangs des 19. Jahrhundert als die „weltbeste Polizei“ anerkannt wurde. Dr. Hans Schober, Präsident der Polizei in Wien, konnte auf Grund dieser Rahmenbedingungen die Gründung der Interpol in Wien im Jahre 1923 verwirklichen. An Hand historisch relevanter Kriminalfälle schilderte ich einige Details der Arbeitsweise der Kriminalpolizei:

Der Mord an dem Mannequin Ilona Faber, die am 15. April 1958 beim Russendenkmal tot aufgefunden wurde, erregte bei der Wiener Bevölkerung große Aufmerksamkeit. Ein verdächtiger Strotter, Johann Gassner, damals dreißig Jahre alt, auf den etliche Indizien passten wie: einschlägige Vorstrafen, Bewegungsprofil, gefundene Fußabdruckspuren, Samenflecken in seiner Unterhose, auffälliger Biss in die Brust des Opfers, der auf seine Täterschaft schließen ließ, reichten aber nicht aus das Geschworenengericht von seiner Schuld zu überzeugen. Gassner wurde von der Mordanklage freigesprochen. Im Jahr 2002 fand dieser Fall seine späte Klärung. Ein Hinweis einer Frau, die ihren verstorbenen Gatten der Ermordung Ilona Fabers bezichtigte, da dieser die Tat am Sterbebett gestanden hätte, konnte durch neue Ermittlungen und moderne wissenschaftliche Methoden widerlegt werden. Gleichzeitig wurde Johann Gassner die Täterschaft zweifelsfrei nachgewiesen. Das Computersimulationsverfahren des Schweizer Gerichtsmediziners Bruschweiler, der in Zusammenarbeit mit dem Gerichtsmediziner Manfred Hochmeister

Für ein volles Haus sorgten die zahlreichen Besucher

das Sicherheitsbüro unterstützte, erbrachte einen schlüssigen Beweis.

An Hand weiterer spektakulärer Kriminalfälle wie: Opernmord 1963, Herrschaft der Wiener Unterwelt 1976-1978, RAF-Terrorismus in Österreich 1976 und 1977, Frauen- bzw. Kindermorde in Favoriten 1988 bis 1990, Causa Lainz der mörderischen Krankenschwestern 1989 bis 1990, Formen der internationalen Kriminalität, „Russenmafia" 1996, italienische Raubmörder 1998 und italienische Bankräuber 1998 wurden die Methoden der Kriminalpolizei bei Nachforschungen, Ermittlungen und Einvernahmen anschaulich dargestellt. Als letztes Fallbeispiel brachte ich den Diebstahl der Saliera vom 11. Mai 2003 im Kunsthistorischen Museum. Der Fall wurde „geklärt“, die Saliera wurde dem Kunsthistorischen Museum 2006 zurückerstattet. Wie aber der Diebstahl tatsächlich erfolgte, blieb im Dunklen.

Die abschließende Diskussion zu Polizei- und Strafprozessreform führte zu der Frage, welche Anforderung an Staatsanwaltschaften, Gericht und Polizei zukünftig gestellt werden. Der Hausherr und Gastgeber Mag. Friedrich Forsthuber, Präsident des Landesgerichtes für Strafsachen Wien, sprach die neuen Rollenbilder und das Selbstverständnis von Justiz und Polizei an. Eine gute Zusammenarbeit zwischen Justiz und Polizei wird aber immer der Schlüssel zum Erfolg bleiben.

• Maximilian Edelbacher

Die dunkle Seite von Wien

Der Sutton Verlag ermöglicht es die spektakulären Kriminalfälle meiner Zeit als aktiver Polizist, später dann als Special Investigator der AVUS GROUP, veröffentlichen zu können. Zwei Ausstellungen, die in Wien in den Jahren 2012 und 2013 veranstaltet werden, sind Motiv für dieses Buch. Die Ausstellung „Die Geschichte des Grauen Hauses und der österreichischen Strafgerichtsbarkeit“ findet vom 14. Juni bis 10. November 2012 im Landesgericht für Strafsachen Wien stattf. Die zweite Ausstellung beschäftigt sich mit dem Thema „Glückspiel“. Diese Ausstellung wird vom Oktober 2012 bis März 2013 im Museum der Stadt Wien gezeigt werden.

Interessenten an diesem Buch wenden sich bitte an unsere Redaktion bzw. das Sekretariat der VKÖ - siehe Impressum

Die Geschichte des Grauen Hauses: Das Buch

Das Landesgericht Wien, von den Wienern liebevoll „Landl“ genannt, hat seine Pforten seit Mitte Juni bis 10. November d.J. für das Publikum geöffnet. Die Geschichte des Hauses und die der österreichischen Strafgerichtsbarkeit sollen wohl in volksnähe gerückt werden und den Ruf der Gerichtsbarkeit als unnahbare Institution verbessern. Anlässlich dieses historischen Rückblicks, den man nur empfehlen kann vor Ort zu besichtigen, hat der Bibliotheksverein des Landesgerichts Wien ein 173 Seiten starkes Buch herausgebracht. Trotz des etwas sperrigen Titels (Die Geschichte des Grauen Hauses und der österreichischen Strafgerichtsbarkeit) birgt das Buch doch interessante und teilweise unbekannte Informationen über die Gerichtsbarkeit im Laufe der letzten Jahrhunderte. Ein wesentliches Kapitel ist spektakulären Prozessen gewidmet.
Die Riege der Autoren des Buches enthält bekannte Namen aus Justiz und Polizei. Auch der Bildungsreferent der VKÖ, Mag. Max Edelbacher, ist vertreten. In seinem Beitrag reflektiert er die Zusammenarbeit zwischen Justiz und Polizei und die auslösenden Faktoren.
Das Buch ist NICHT im Buchhandel erhältlich, ist aber um Euro 12,- im Landesgericht während der Ausstellungszeiten erhältlich.

Das Recht der österreichischen Berufsdetektive

samt Vorbereitung auf die staatliche Befähigungsprüfung
Peter Pokorny

Berufsdetektive ermitteln in Strafsachen, beschaffen Beweise für Gerichtsverfahren und leisten bewaffneten Personenschutz.
Sie fahnden nach untergetauchten Straftätern oder Schuldnern, halten Tatverdächtige an und erstatten Strafanzeigen an Polizei und Staatsanwaltschaften. Da sie dabei immer wieder in die Grundrechte Dritter eingreifen, ist ein hohes Maß an juristischem Wissen wichtig. Das „Recht der Österreichischen Berufsdetektive“ ist Lehrbuch und Nachschlagewerk in einem und darüber hinaus die Basis für die Vorbereitung auf die staatliche Befähigungsprüfung.
Aus dem Inhalt:

- Der Berufsdetektiv als Arbeitgeber
- Datenschutz und Verschwiegenheit
- Erhebungs- und Ermittlungswesen
- Beweisarbeit und Gerichtswesen
- Notwehr und Festnahme
- Berufsdetektive und Kaufhausüberwachung
- Die Sprache der Juristen, Arbeiten mit Rechtsquellen
- Schriftliche und mündliche Prüfungsfragen

Peter Pokorny ist seit 1992 als Berufsdetektiv tätig, er ist stellvertretender Präsident des Europäischen Detektiv-Verbandes (EURODET) und dessen Lehrbefugter für Rechtskunde.
Zielgruppen: Berufsdetektive und Berufsdetektivassistenten, Auszubildende und Prüfungskandidaten.

MANZ‘scher Verlag Wien, 8/2010
ISBN-13: 978-3214007195
€ 48,-

Sicherheitsverwahrung

– wissenschaftliche Basis und Positionsbestimmung
Was folgt nach dem Urteil des Bundesverfassungsgerichts vom 4.5.2011?

Die deutsche Rechtslage zum Thema Sicherheitsverwahrung wurde durch die Urteile des Europäischen Gerichtshofes für Menschenrechte, 2009, und des Deutschen Bundesverfassungsgerichtshofes, 2011, massiv erschüttert, da die Maßregeln der Sicherheitsverwahrung als menschenrechtswidrig verworfen wurden. Hintergrund dieser Entwicklung war die Kritik an der unverhältnismäßigen Steigerung bei der Anwendung der Maßregeln der Sicherheitsverwahrung. Sicherheitsverwahrung wurde aus der Sicht der beiden Gerichte als Strafe, Verletzung des Grundsatzes der Verhältnismäßigkeit, des Vertrauensschutzgebotes und des Abstandsverbotes qualifiziert, da kein freiheitsorientiertes Gesamtkonzept bei den Maßregeln der §§ 63 – 66 StGB und beim Therapieunterbringungsgesetz erkannt werden konnte. Der Europäische Gerichtshof für Menschenrechte beurteilte die Beseitigung der 10-Jahresgrenze als einen Verstoß gegen das Rückwirkungsverbots des Art. 7 EMRK. Das deutsche Strafgesetzbuch kannte bis dahin die primäre Sicherheitsverwahrung, § 66 StGB, die vorbehaltene Sicherheitsverwahrung, § 66a StGB und die nachträgliche Sicherheitsverwahrung 66b StGB.
Hans-Jörg Albrecht stellt im Buch fest, dass infolge spektakulärer Vorfälle ab Mitte der 90-iger Jahre der Focus auf Sexual- und Gewalttäter konzentriert wurde. Damit rückten die Maßregeln der Sicherheitsverwahrung in die rechtspolitische Aufmerksamkeit.
Es wird aber auch befürchtet, dass die gesetzliche Neuregelung in Deutschland, die bis Mai 2013 erfolgen muss, einen Etikettenschwindel statt eines echten Risk-Need-Responsivity Ansatzes bringen könnte. • Maximilian Edelbacher

Die Medizinisch Wissenschaftliche Verlagsgesellschaft publizierte das Buch 2012 in Berlin mit zuvor zitiertem Titel von J.L. Müller, N. Nedopil, N. Saimeh, E.Habermeyer, P. Falkai als Herausgeber mit Beiträgen H.J. Albrecht, H.G. Bamberger, A. Boetticher, B. Borchard, A. Dessecker, V. Dittmann, E. Habermeyer, C. Huchzermeier, J. Kinzig, M. Koller, H.-L. Kröber, J. L. Müller, N. Nedopil, W. Pfister, J. Sauter, G.Stolpmann, F. Urtbaniok, K. Vohs, B. Völlm, T. Voß und T. Wolf.