Situative Prävention von Cybercrime: ein chancenreicher Bekämpfungsansatz

Prof. Dr. Pieter Hartel

Vielen Dank, Herr Prof. Dr. Kerner, für die gelungene Einführung, die ich selbst nicht besser hätte machen können. Ich danke auch dem Bundeskriminalamt für meine Einladung als Vortragsredner. Ich bin überwältigt in Anbetracht der großen Zahl von Zuhörern, die sich hier eingefunden haben, um meinem Vortrag zuzuhören. Ich werde versuchen, dem gerecht zu werden.

Das Thema meines Vortrags ist, wie Sie sehen können, die „Situative Prävention von Cybercrime" und ich werde versuchen, Ihnen im Verlauf meiner Ausführungen zu erklären, was damit gemeint ist. Aber bevor ich beginne, seien noch folgende Anmerkungen gestattet: Es geht hier nicht um die Art von Cybercrime, über die am Vormittag gesprochen wurde. Es geht hier nicht um Cyberspionage. Es geht auch nicht um all die Großereignisse, die jeden Tag Schlagzeilen machen, sondern es geht um das Alltagsgeschäft. Da dies so allgegenwärtig ist, lohnt sich eine nähere Betrachtung, denn eine Vielzahl kleiner Vorfälle besitzt in der Summe auch ein großes Schadenspotenzial. Deshalb ist es auch lohnend, die Aufmerksamkeit auf einfache Erscheinungsformen der Kriminalität zu richten. Lassen Sie mich dies anhand einiger Beispiele beschreiben, die wir bisher noch nicht behandelt haben:

Der folgende Fall ereignete sich im Jahr 2000 in Australien: Ein Angestellter ärgerte sich über seinen Chef, weil dieser ihm einen unbefristeten Arbeitsvertrag verweigerte. Er wurde daraufhin entlassen, was ihn sehr verärgerte. Zuständig war er für die Kläranlage in Queensland. Ausgelöst durch seinen Ärger, begann er, die Einrichtungen zu manipulieren. Man hatte vergessen, seine Zugangsberechtigungen zu widerrufen mit der Folge, dass er immer noch seinen Benutzernamen und sein Passwort besaß. Natürlich war das ein großer Fehler, aber Menschen machen nun einmal Fehler. Die betreffende Person hat dann Millionen Liter ungeklärtes Wasser auf die städtischen Parkanlagen geleitet, und das nicht nur einmal, sondern 46 Mal, und zwar über einen Zeitraum von mehreren Monaten, in denen er nicht gefasst werden konnte. Letztlich gelang es, ihn dingfest zu machen, aber zunächst einmal war man ganz offensichtlich gezwungen, knietief durch Klärschlamm zu waten, ohne dass der

Verursacher gestoppt werden konnte. Bei diesem Fall handelt es sich nach meiner Auffassung um eine Form von Cybercrime. Ein weiterer, m. E. interessanter Beispielsfall liegt bereits einige Jahre zurück und ereignete sich in Moskau. Ein gelangweilter russischer Hacker wollte seine Muskeln spielen lassen und seine Fähigkeiten an einer großformatigen digitalen Werbetafel im Zentrum der Hauptstadt erproben. So hackte er sich in das entsprechende Programm, um auf der Videotafel Pornos abzuspielen und zu testen, was dann mit dem Verkehr passiert. Sie können sich vorstellen, dass das Ganze sehr unerfreulich war, denn selbst zu den besten Zeiten ist das Verkehrsaufkommen in Moskau nicht gerade angenehm, und diese Aktion machte das Ganze noch viel schlimmer. Für sein kleines Abenteuer wurde der Hacker verurteilt und für eineinhalb Jahre aus dem Verkehr gezogen.

Ein weiterer Fall beschäftigte die europäische Polizei, insbesondere die niederländischen Kollegen, die sich vor einigen Jahren sehr lange mit dem Betreiber eines Bot-Netzes, dem sogenannten Bredolab-Bot-Net, befassen mussten, um dieses unschädlich zu machen. Dabei handelt es sich zugleich um den ersten Cyber-Kriminellen, der in Armenien, seinem Geburtsland, hinter Schloss und Riegel sitzt, was als großer Erfolg zu werten ist. Wir haben es mit einer großen Bandbreite von Cyberkriminalität zu tun; einige Fälle machen große Schlagzeilen und verursachen große Schäden, und andere sind etwas weniger einschneidend.

Meine Hypothese lautet, dass dies etwas mit Gelegenheiten zu tun hat. Betrachtet man das Beispiel des russischen Hackers, so hat dieser für sich eine Gelegenheit entdeckt und sie genutzt, und es gab nichts, was ihn davon abgehalten hätte. Für diesen großen Spaß rechnete er mit einem geringen Risiko und sah somit keinen Grund, von seinem Vorhaben abzulassen. Meine Hypothese lautet also, dass der Cyberspace einfach viele Tatgelegenheiten bietet.

Herr Prof. Dr. Kerner hat gerade die Theorie der Routineaktivität erwähnt. Es braucht nur einen motivierten Straftäter und ein geeignetes Angriffsziel, und derer gibt es viele im Cyberspace. Der zur Tat entschlossene Straftäter glaubt, dass er sich einem geringen Risiko aussetzt, wenn er seine Taten aus der sicheren und geschützten Umgebung seiner eigenen vier Wände heraus verübt. Die angegriffenen Personen kennen das Risiko nicht; viele benutzen schwache Passwörter oder verhalten sich so, wie es eigentlich nicht sein sollte, oder beides. Und als professionelle Sicherheitsdienstleister geben wir Verhaltensempfehlungen, aber niemand kann für die Missachtung unserer Warnungen belangt werden. Und sowohl auf Seiten der Täter als auch auf Seiten der angegriffenen Personen stellt sich die Frage der Risikobewertung, die nicht immer so beantwortet wird, wie sie sollte. Es gibt in unserer Welt eine Vielzahl von Tatgelegenheiten, die uns Anlass zur Sorge geben sollten. Und aus Erfahrung wissen wir, dass Gelegenheit Diebe macht. Auch ein ansonsten braves Kind bedient sich eigenmächtig an der Keksdose, wenn es hierzu die Gelegenheit erhält. Und vielleicht waren wir als Kinder auch nicht anders. Ich zumindest kann mich da nicht ausnehmen. Das ist keineswegs schön, entspricht aber der menschlichen Natur. Man mag dies in Abrede stellen, aber ist es besser, dies zur Kenntnis zu nehmen und in Bezug auf die Tatgelegenheiten Maßnahmen zu ergreifen. Versuchen wir einmal, von der Annahme auszugehen, dass sich Menschen ihren Gewohnheiten entsprechend verhalten, und lassen Sie uns dann versuchen, ihnen das Ergreifen von Gelegenheiten einfach zu erschweren. Zu diesem Zweck müssen wir uns die Theorie der Tatgelegenheiten anschauen.

Es gibt 5 Prinzipien der Reduzierung von Tatgelegenheiten:

1. Erhöhung des Aufwandes; das klassische Beispiel hierfür ist die Verwendung besserer Türschlösser, was in der Regel funktioniert, sofern die Tür tatsächlich verriegelt wird.

2. Erhöhung des Entdeckungsrisikos; Überwachungskameras können hierfür als offenkundiges Beispiel dienen und deren Nutzen konnte in einigen Fällen belegt werden.

3. Reduzierung des Nutzens; wenn der ungünstige Fall eintritt und privates Eigentum gestohlen wird, wird dies im Falle der eindeutigen Kennzeichnung als Privateigentum - z. B. durch Eingravieren des Kfz-Kennzeichens in die Fenster Ihres Fahrzeugs - zu einem weniger attraktiven Angriffsziel, weil es auf diese Weise schwerer ist, das Diebesgut weiter zu veräußern, wodurch die Tatgelegenheit eingeschränkt wird.

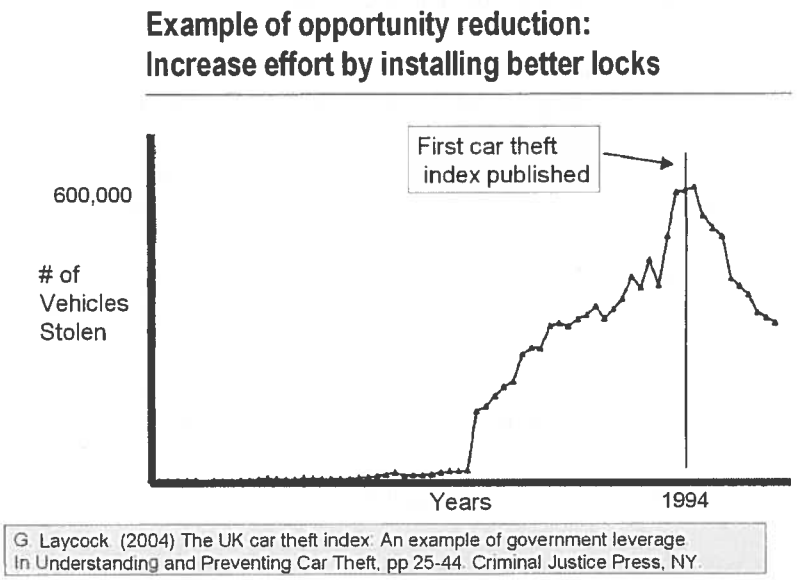
4. Reduzierung des Anreizes für die Tatbegehung.

5. Reduzierung von Entschuldigungsgründen.

Somit steht eine Reihe von Möglichkeiten zur Reduzierung von Tatgelegenheiten zur Verfügung.Bemerkenswert ist, dass die Tauglichkeit dieser fünf Prinzipien in einer Vielzahl von Fällen nachgewiesen wurde und viele Forschungsarbeiten belegen, dass die Beachtung dieser Prinzipien in der Tat die Gelegenheiten zur Begehung einer Straftat reduziert.

Im Bereich des US-Justizministeriums gibt es das Center for Problem-Oriented Policing (Zentralstelle für Problemorientierte Polizeiarbeit), das eine Sammlung von Eingriffsmaßnahmen vorhält, die auf den genannten Prinzipien basieren und die nachweislich erfolgreich zur Reduzierung von Tatgelegenheiten beigetragen haben.

Wenn wir das Gesagte als Grundannahme betrachten, dann könnten wir uns jetzt die Frage stellen, warum wir einen so erfolgreichen Ansatz nicht auf den Bereich Cybercrime übertragen? Das ist eine Frage, die ich mir selbst vor einigen Jahren gestellt habe. Zuvor sei aber noch ein weiteres Beispiel für die Wirksamkeit dieses Ansatzes angeführt.



Die obige Graphik zeigt die Anzahl der zum Ende des letzten Jahrhunderts im Vereinigten Königreich gestohlenen Fahrzeuge. Dieser Graphik lässt sich entnehmen, dass bis zu einem bestimmten Zeitpunkt ein Anstieg der Anzahl gestohlener Fahrzeuge verzeichnet wurde. Verantwortlich hierfür waren zum einen gestiegene Zulassungszahlen, zum anderen aber auch eine wachsende Zahl von Diebstahlsfällen. In den achtziger Jahren ließ sich mit dem Schlüssel eines Ford Taunus wahrscheinlich auch jeder andere Fort Taunus auf der Straße öffnen. Dieses Beispiel einer außerordentlich schwachen Sicherung, aus der sich ein Übermaß an Tatgelegenheiten ergab und bei denen Täter der Versuchung nachgegeben haben, ist ein Beleg für unsere Feststellungen. Unter dem Eindruck des damaligen Sicherheitsdefizits im Bereich der Kraftfahrzeuge erkannte die Regierung des Vereinigten Königreichs Handlungsbedarf und fasste einen sehr interessanten Beschluss. Dieser bestand in der Veröffentlichung eines Index' gestohlener Kraftfahrzeuge. Wenn Fahrzeughersteller dann feststellen mussten, dass die eigene Marke und das Vorzeigemodell ganz oben auf diesem Index standen, dann war das keine gute Werbung in der Öffentlichkeit. Man wollte nicht auf dieser Liste sein, weil die eigene Kundschaft dann geneigt war, zu denken: „Wenn ich dieses Marke und dieses Modell kaufe, dann wird es umgehend gestohlen, weshalb ich mich besser für ein anderes entscheide."

Das war ein sehr starker Handlungsanreiz für die Fahrzeughersteller, ihre Fahrzeuge in der Folge mit besseren Sicherungsvorrichtungen auszustatten. Und siehe da, nach Veröffentlichung dieses Index' gestohlener Fahrzeuge zeigte sich, dass die Diebstahlszahlen zurückgingen. Für den Rückgang der Zahlen könnte es natürlich auch andere Gründe geben. Es könnte mit dem Ölpreis zusammenhängen oder mit sinkenden Verkaufszahlen, aber die Wissenschaftler, die in diesem Bereich geforscht haben, haben sich sehr darum bemüht, die Lage umfassend zu berücksichtigen und sind zu dem Schluss gekommen, dass der Rückgang der Kfz-Diebstahlszahlen mit hoher Wahrscheinlichkeit auf die Installation besserer Sicherungstechnik zurückzuführen ist. Das sind Maßnahmen, die funktionieren - vielleicht auch im Bereich Cybercrime. Betrachten wir nun die von uns durchgeführten Untersuchungen.

Die selbst gestellte Aufgabe bestand in der Beantwortung der Frage, wie viele der Maßnahmen zur Reduzierung von Tatgelegenheiten tatsächlich im Cyberbereich ausprobiert worden sind und wie wirksam sie waren. Zunächst wurde, wie in der Wissenschaft üblich, eine Auswertung der vorhandenen Literatur durchgeführt, d.h. eine Auswertung der gesamten Literatur in den Bereichen Informatik und Verhaltensforschung, um entsprechende Belege zu finden. Das Resultat war im Grunde gleich null - ein sehr ernüchterndes Ergebnis. Auf der einen Seite gibt es einen Schatz vielversprechender Forschungsergebnisse und auf der anderen Seite das zu lösende Problem, und keiner hat beides bisher miteinander in Verbindung gebracht. Es gibt nur eine kleine Ausnahme, und zwar Forschung in Bezug auf die Bekämpfung von Phishing; hier gibt es Belege für die Wirksamkeit der in Rede stehenden Maßnahmen. Aber da wir alle täglich Phishing-E-Mails erhalten und dies gewiss keine Einzelfälle sind, kann dieses Problem gewiss noch nicht als gelöst gelten, sondern besteht ohne Zweifel größtenteils fort. Die wesentliche Folgerung lautet unbestreitbar, dass dies noch Terra incognita ist und genau deren Erforschung haben sich meine Kollegen und ich verschrieben.

Ich möchte Ihnen daher kurz über drei Versuche berichten, mit denen wir versucht haben, mehr über Tatgelegenheiten und deren Reduzierung herauszufinden.

Der erste Teil ist eine klassische Kriminalaktenauswertung mit dem Ziel, herauszufinden, wie viel Cybercrime es tatsächlich gibt. Das ist zum Einstieg stets ein guter Ansatz, der auch ein sehr interessantes Ergebnis erbracht hat.

Bei dem zweiten Experiment handelt es sich um ein Musterbeispiel für die Schaffung von Tatgelegenheiten. Gemeint sind soziale Netzwerke für Sporttreibende im Internet. Das Experiment offenbarte deren teilweise sehr naive Nutzung, wozu im weiteren Verlauf ergänzende Ausführungen folgen.

Bei dem dritten Experiment ging es darum, mit Hilfe des "social engineering" in den Besitz fremder Büroschlüssel zu gelangen, was erstaunlicher Weise sehr gut gelang. Dies sollte ohne Zweifel vermieden werden, da hierdurch jede noch so gute Sicherheitsstrategie ausgehebelt wird.

Die erste Fallstudie bestand in der Analyse von 809 Kriminalakten der fünf niederländischen Polizeiregionen mit einer Grenze zu Deutschland. Der Grund für die Auswahl dieser Polizeien liegt darin, dass sich unsere Einrichtung dort befindet. Dies erleichterte den Zugang zu den kriminalpolizeilichen Akten. Die so zu untersuchende Fragestellung lautete: Wie groß ist der Cyberanteil in diesen Vorgangsakten? Berichten anderer Forscher zufolge macht Cybercrime ein Prozent der Kriminalität aus. Das ist die in offiziellen Polizeistatistiken genannte Zahl, die aus der Anfangszeit der hier beschriebenen Forschungsarbeit stammt. Es bestand jedoch die Auffassung, dass ein Prozent nicht zutreffend sein kann; 96 Prozent der Bevölkerung in den Niederlanden nutzen heute ständig das Internet. Wie kann es nun sein, dass eine Sache, die so umfassend Bestandteil des täglichen Lebens ist, keinen Niederschlag in der Kriminalstatistik findet? Der Schluss liegt nahe, dass hier eine Unstimmigkeit besteht. Und es galt herauszufinden, womit das zusammenhing.

Wie bereits gesagt ging es um die Betrachtung von Allgemeinkriminalität, d.h. mit Einbruchdiebstahl in zwei Ausprägungsformen - Wohnungseinbruch und Einbruch in Geschäftsräume. Außerdem wurden Fälle von Bedrohung und Betrug ausgewertet. Bezogen auf jede Kriminalitätskategorie wurden etwa 300 Fallakten analysiert, also insgesamt 900 Fallakten. Die Analyse erfolgte mit größtmöglicher Sorgfalt. Jede Akte wurde sehr genau studiert und anhand einer langen Liste von Kriterien ausgewertet. Dies erbrachte folgendes Ergebnis: Es gab 135 Fälle von Einbruchdiebstahl und nur in 3 Prozent der Fälle wurde in irgendeiner Form Informations- und Kommunikations-(IuK-)Technologie eingesetzt. Dabei handelte es sich um E-Mails oder Mobiltelefone etc., wie sie im Arbeitsalltag genutzt werden. Dies galt dann in dem jeweiligen Fall von Einbruchdiebstahl als Teil des Modus Operandi (M.O.). Der prozentuale Anteil ist also gering. Was den Einbruchdiebstahl zum Nachteil von Geschäften angeht, so gab es hier keinerlei Hinweis auf die Nutzung von ICT im Modus Operandi. Ergänzend ist jedoch festzuhalten, dass es aufgrund vieler Überwachungskameras durchaus einen hohen IuK-Anteil gab. So konnten die meisten Einbrüche in Geschäftsräume aufgeklärt werden, weil es dank der Überwachungskameras Beweismaterial gab. Aber da Überwachungskameras nicht Bestandteil des M.O. ist, wurden diese Fälle für die Auswertung nicht gezählt.

Bei den Bedrohungsfällen kam IuK mit einem Anteil von 16 Prozent zum Einsatz. Häufig kommt es gerade zwischen Familienmitgliedern oder Geschäftspartnern oder generell im Kontext zwischenmenschlicher Beziehungen zu Bedrohungen, also etwa dem Versenden von E-Mails mit bösartigem Inhalt, so dass der Anteil von vornherein schon sehr hoch ist.

Bei Betrugstaten ist es so, dass in fast der Hälfte aller Fälle IuK Teil des M.O. war. Dabei geht es um Betrug bei Online-Auktionen, wo jemand etwas bestellt, bezahlt und keine Ware erhält oder umgekehrt, sowie Betrug im Zusammenhang mit Online-Banking und dergleichen.

Wenn man einen aggregierten Anteil von IuK an allen Fällen betrachtet, liegt dieser IuK-Anteil bei 20 Prozent, und das ist deutlich mehr als ein Prozent. Das hängt natürlich damit zusammen, wie gemessen wird. Wir sind aber der Auffassung, dass wir eine bessere Messmethode gefunden haben, unabhängig von der örtlichen Gesetzgebung, denn bei der Messung von Cybercrime nach der klassischen Methode schlägt man die im Strafgesetzbuch enthaltene Definition von Cybercrime nach und zählt dann die Fälle in der Kriminalstatistik.

Das ist allerdings nicht die hier angewandte Methode. Wir haben uns die tatsächliche Auswirkung der Technik angeschaut und gelangten so zu der ersten überraschenden Erkenntnis. Die zweite Überraschung ergab sich aus Zeitungsberichten, denen zufolge Cybercrime einen hohen Organisationsgrad aufweisen soll. Es gibt einen Bericht der UNODC, demzufolge 90 % von Cybercrime Organisierte Kriminalität ist.

Hierzu wurden Fälle von Alltagskriminalität betrachtet sowie bei den Betrugsfällen Verdächtige, die festgenommen wurden und bei denen entsprechende Informationen in den Fallakten zu finden waren. Dabei wurde festgestellt, dass im Falle der Nutzung von IuK 95 Prozent der Täter alleine arbeiten, die Taten mithin keineswegs Fälle von organisierter Kriminalität sind. Es kann sich dabei um Fälle handeln, in denen jemand vielleicht seine ehemalige Freundin mit einer E-Mail bedroht oder auch eine schwerwiegendere Tat begeht, was jedoch keineswegs organisierte Kriminalität darstellt. Viele der Täter haben keine kriminalpolizeilichen Erkenntnisse, was als ergänzender Hinweis dafür dienen mag, dass Organisierte Kriminalität nicht vorliegt. Alle Täter gehen einem regulären Beruf nach und agieren auch nicht weltweit, sondern an ihrem Heimatort. Somit ergibt sich ein ganz anderes Bild als das, das man bei der Betrachtung hochkarätiger Fälle erhält. Und auch das ist Teil der

Realität von Cybercrime. Wir sind der Auffassung, dass es sich dabei um eine recht interessante Feststellung handelt. Soll dieses Phänomen nun reduziert werden, dann muss man dieser Feststellung Rechnung tragen.

Lassen Sie mich nun zu der zweiten Fallstudie kommen. Sie wissen alle, was ein soziales Netzwerk im Internet ist, also Facebook, Linked-In etc., aber es gibt auch spezialisierte soziale Netwerke im Internet für Leute, die einen bestimmten Sport treiben. Dabei geht es etwa um Läufer, die ein GPS-fähiges Aufzeichnungsgerät haben und nach Beendigung eines Laufs diesen automatisch hoch laden. Benutzt wurden hier die Daten eines Studenten, der diese freundlicherweise zur Auswertung und für Präsentationszwecke zur Verfügung stellte.

Anhand der Daten lässt sich herausfinden, wo dieser Student wohnt. Das GPS-Gerät wird eingeschaltet, wenn man die Haustür passiert. Anschließend wird der Lauf absolviert und das Gerät ausgeschaltet, wenn der Läufer wieder zuhause ankommt oder, um es noch ein wenig interessanter zu machen, das Gerät wird schon ein wenig früher ausgeschaltet, weil man verhindern will, dass Aufwärm- und Auslaufphase die Laufstatistik verzerren.

Es lässt sich nun aber herausfinden, wo jemand wohnt, und das ist die frohe Botschaft für Straftäter. Dieser muss nur die Website aufrufen, auf der die Läufe aufgezeichnet werden; zum einen weiß der Täter dann, wo das Opfer wohnt, und zum anderen, wann es sich außer Haus befindet. Das sind ideale Voraussetzungen für einen Wohnungseinbruch. Es gibt einen Slogan, der lautet "auch Diebe haben Facebook" und ich würde ergänzen "Diebe kennen auch die Seite RunKeeper".

Untersucht wurden insgesamt 513 Profile, wobei folgendes festgestellt wurde: Die Analyse der Ergebnisse männlicher Läufer (313 von 513) ermöglichte in 36 Prozent der Fälle die Feststellung des Wohnorts. Bei den weiblichen Läuferinnen ergab sich sogar noch ein höherer Prozentsatz. Wenn man das vergleicht mit der Prozentzahl, die bei den weiter verbreiteten sozialen Netzwerken ermittelt wurde, dann liegt diese deutlich niedriger, weil Leute bei Facebook sehr viel zurückhaltender mit der Offenlegung ihrer Namen und Anschriften sind als im Falle der Nutzer spezialisierter Netzwerke. Die meisten Leute sind sich dieser Risiken einfach nicht bewusst und ich denke, dies erzeugt eine große Zahl von Gelegenheiten, über die wir nachdenken sollten.

Bei der letzten Fallstudie sind wir selbst aktiv geworden und wollten herausfinden, inwieweit Menschen Sicherheitsvorkehrungen befolgen, die ihnen von einer Hausgemeinschaft vorgegeben sind. Wir haben für unsere Büros elektronische Schlüssel, die keinesfalls in fremde Hände gelangen dürfen. Wir haben hierzu der Hälfte der Bewohner eines Mehrparteienhauses spezielle Schlüsselanhänger ausgehändigt, auf denen geschrieben stand „Gib mich nicht an einen Fremden weiter“. Zwei Wochen später entsandten wir eine Gruppe von Studenten eines Masterstudiengangs in das Wohnhaus. Die Studenten sollten mit einer erfundenen Geschichte versuchen, in den Besitz möglichst vieler Schlüssel zu gelangen. Der Vorwand hierfür war recht einfach konzipiert: Wir benutzten hierzu ein Kästchen mit einer Batterie und einem Schalter verbunden mit einer eingebauten LED, also eine wenig komplizierte Vorrichtung. Wenn der Schlüssel nun in das Kästchen eingeführt wird, leuchtet die LED auf.

Die Studenten hatten die Vorgabe, zu behaupten, dass es bedauerlicherweise Probleme mit den elektronischen Schlüsseln gebe – zur Erinnerung: das rechtfertigt den IuK-Bezug – und dass die Funktionalität des Schlüssels überprüft werden müsse. Die Stundenten sollten dann sagen, dass der Schlüssel defekt sei und repariert werden müsse. Teil der fingierten Geschichte war zudem, dass die Schlüssel jeden Tag von neuem aktiviert werden müssen, da sie ein digitales Zertifikat beinhalten, dessen Gültigkeit vermeintlich nach 24 Stunden abläuft. Wenn man morgens zur Arbeit geht und das Büro betritt, wird der Schlüssel aktiviert. Nach der Versuchsanordnung sollten die Studenten die Schlüssel dann an sich nehmen, um sie im Erdgeschoss wieder zu aktivieren. Das stand im Widerspruch zu den Sicherheitsvorschriften der Bewohnergemeinschaft, denn die Bewohner sollten den Schlüssel ja nicht aus der Hand geben, sondern die erneute Aktivierung persönlich vornehmen. Sie können sich vorstellen, dass unsere Masterstudenten von dieser Art der Versuchsgestaltung begeistert waren. Zudem erhielten sie Credits für ihren Einsatz. Mittels „Social Engineering“ die Schlüssel anderer Leute entwenden und hierfür obendrein Credits erhalten, ist natürlich eine feine Sache.

Die Ergebnisse sind wie folgt: Es gab 74 Zielpersonen, die angesprochen wurden. Die Hälfte der Zielpersonen gab ihren Schlüssel heraus, die andere Hälfte nicht. Dabei handelt es sich nicht um einen Auswertefehler. Tatsächlich hat sich eine Pattsituation von 50 zu 50 ergeben. Das kommt nicht sehr häufig vor, dieses Ergebnis ist aber korrekt.

Noch interessanter ist der Umstand, dass die Personen gewarnt wurden, indem sie den Schlüsselanhänger mit der Aufschrift erhielten "Don't give this key away", denn dies hatte signifikante Auswirkungen auf das Verhalten: 38 Prozent gaben ihren Schlüssel heraus, während in der Kontrollgruppe, die den Schlüsselanhänger *nicht* erhielt, 62 Prozent den Schlüssel herausgaben. Es ist also tatsächlich möglich, aktiv zur Reduzierung von Tatgelegenheiten beizutragen. Bei den Personen, mit denen dieser Versuch durchgeführt wurde und die tatsächlich auf diese unglaubliche Geschichte hereinfielen, handelte es sich um Elektroingenieure. Man stelle sich einmal vor, wie sich Nicht-Ingenieure in einer solchen Situation verhalten. Wie dem auch sei, dieser Versuch war zwar hilfreich, aber nicht hilfreich genug, denn das Problem ließ sich zwar halbieren, aber ein Großteil blieb bestehen. Das bedeutet, dass noch viel zu tun ist.

Damit bin ich bei meinen Schlussfolgerungen angelangt. Eine der wesentlichen Schlussfolgerungen, die sich festhalten lassen, lautet: Cybercrime speist sich aus Gelegenheiten, und da sie alle Lebensbereiche durchdringt, hat Cybercrime gewissermaßen den Charakter von Alltagskriminalität.

Festgestellt wurde auch, dass Frauen kriminell wesentlich aktiver sind, wenn der Cyberraum eine Rolle spielt, und wir sind der Auffassung, dass dies damit zu tun hat, dass sie sich sicherer fühlen, wenn sie aus der sicheren Umgebung ihrer eigenen vier Wände agieren können. Sie sind z.B. bereit, jemanden bei einer Online-Auktion zu betrügen, während es in der realen Welt größere Risiken gibt, weshalb sie hier möglicherweise weniger geneigt sind, eine solche Tat zu begehen. Das bedeutet wiederum, dass wesentlich mehr Leute kriminell werden, und das ist ein Alarmsignal. Dies zeigt aber auch, in welche Richtung wir uns begeben müssen, wenn wir uns um Vorbeugung bemühen. Einer der Schlüsselaspekte ist das „Social Engineering“. Wenn man eine gute Geschichte hat, kann man fast alles erreichen. Psychologie ist ein wesentlich wichtigeres Instrument als Technologie, um dem hier in Rede stehenden Problem zu begegnen.

Um das Problem von Cybercrime zu lösen, muss man es vielleicht gar nicht als technisches Problem sehen, sondern vielmehr als psychologisches. Und das ist ein Aspekt, den Techniker nur schwer zu akzeptieren bereit sind, aber meiner Auffassung zufolge handelt es sich hierbei um eine Tatsache.

Hier wurde der Versuch unternommen, der Frage nachzugehen, ob die Reduzierung von Gelegenheiten auch im Cyberraum funktioniert. Endgültige Antworten sind noch nicht gefunden und wie bereits gesagt war auch die einschlägige Literatur nicht ergiebig. Meiner Auffassung nach liegt hier aber ein großes Potenzial und es ist zu hoffen, dass ein oder zwei der hier Anwesenden bereit sind, mit anzupacken und diese Forschung weiter voranzutreiben.

Vielen Dank für Ihre Aufmerksamkeit. Vielen Dank nochmals an das Bundeskriminalamt für die Einladung. Und ich hoffe, Sie haben mir gerne zugehört.