SKP INFO

4 | 2016

Thema
Internetkriminalität

Liebe Leserin, lieber Leser


SKP

Die Energie, die aufgewendet wird, um im Internet Menschen zu bestehlen, zu belügen, ihnen Gefühle vorzugaukeln oder sie mit Hasstiraden zu überschütten, scheint unendlich zu sein.

Im Interview mit Stéphane Koch wurde mir einmal mehr bewusst, dass Ausbildung einer der Schlüssel für eine erfolgreiche Prävention von Internetkriminalität ist. Medienkompetenz kann mithelfen, sich adäquat zu schützen, nicht alles zu glauben, was man sieht und liest, und zu verstehen, wie das Internet und die Sozialen Medien funktionieren. Der Wissensstand der Anwenderinnen und Anwender sollte daher deutlich verbessert werden.

Die Stadtpolizei Zürich hat den Austausch mit der Bevölkerung gezielt über die Sozialen Medien verstärkt. Die Öffentlichkeit kann in den Sozialen Medien die beiden iCoPs Jean Patrick und Eleni Moschos begleiten, die ihre tägliche Polizeiarbeit auf Facebook und Twitter beschreiben. Beide iCoPs stehen so täglich in regem Kontakt mit Jugendlichen und jungen Erwachsenen aus Zürich und Umgebung. Dadurch wird die Arbeit der Polizei transparenter, was das Vertrauen der Bevölkerung in ihre Polizei positiv verstärkt.

Wir wünschen Ihnen alles Gute
im Jahr 2017.

Martin Boess
Geschäftsleiter SKP

Aktuelle Situation und Tendenzen der Kriminalität im Internet

Ein Interview mit Stéphane Koch

Sehr geehrter Herr Koch
Sie haben eine eigene Webseite unter dem Namen www.intelligentzia.ch und Ihre Dienstleistungen fassen Sie wie folgt zusammen: «Beratung und Ausbildung in Wirtschaftsinformation und Informationsstrategien, Digitale Strategien und Soziale Netzwerke sowie Informationssicherheit». Eindrücklich sind auch Ihre verschiedenen Ausbildungen, die sich alle auf das Thema «Digitale Medien» beziehen. Sie sind somit der ideale Interviewpartner, wenn wir uns über das Thema «Kriminalität im und mit dem Internet» unterhalten wollen, dies natürlich mit Fokus auf kriminalpräventive Massnahmen und die Strafverfolgung. Aber vorerst eine allgemeine Frage:

Wie unterscheidet sich «normale» Kriminalität von Internetkriminalität resp. wie hat das Internet die Kriminalität verändert?
Der Unterschied liegt vor allem auf der Ebene der Entmaterialisierung unserer Gesellschaft, das heisst, der Übergang von Kriminalität in der realen Welt zur Cyberkriminalität ist fliessend – in der Cyberkriminalität werden Formen der Kriminalität adaptiert, die auch in der realen Welt vorkommen. Viele kriminelle Aktivitäten, die mit Hilfe von Informations- und Kommunikationstechnologien (IKT) bzw. im Internet stattfinden, sind in der realen Welt verankert (etwa durch den Gebrauch eines Server, eines Computers oder eines Mobilgeräts) und damit steht auch der Gerichtsstand fest, der sich durch den physischen Ort bestimmt, an dem der Server oder der Computer steht.

Der grösste Unterschied zwischen herkömmlicher und Cyberkriminalität liegt aber in der Asymmetrie zwischen den verhältnismässig geringen Mitteln, die für eine cyberkriminelle Handlung benötigt werden, und den grossen Auswirkungen, die sie entweder in finanzieller Hinsicht oder in Bezug auf die Anzahl der Personen oder Unternehmen, die von einer einzelnen Handlung betroffen sind, haben. Eine andere Form der Asymmetrie liegt auf der Ebene der Bekämpfung von cyberkriminellen Handlungen. Wenngleich es wenig Mittel braucht, um cyberkriminelle Handlungen zu organisieren und durchzuführen (z. B. Online-Betrug, Cyberattacken, Cyberextortion), so braucht es von Seiten der betroffenen Organisationen und Behörden enorme Mittel, um diese Handlungen zu bekämpfen, sei dies nun in Form von Arbeitskräften, von Zeit oder auf der technischen Ebene. Zudem ist es auf juristischer Ebene sehr schwierig. Die realen Orte der Organisation und der Durchführung einer cyberkriminellen Handlung, oder an denen sich die Opfer aufhalten, müssen nicht zwingend die gleichen sein, sie können über verschiedene geografische Zonen auf der Welt


zvg

Stéphane Koch,
Berater und Ausbilder in den Bereichen Kommunikation und Digitale Strategien. Spezialist in Informationssicherheit und Digitale Reputation sowie Soziale Netzwerke.

ascyther5/123RF

«In der Cyberkriminalität werden Formen der Kriminalität adaptiert, die auch in der realen Welt vorkommen.»

verteilt sein, und es kann nicht immer von Rechtshilfeabkommen profitiert werden. Ein grosser Unterschied liegt auch darin, dass die Cyberkriminellen ihre potenziellen Opfer zuhause angreifen können, ohne in ihre Wohnungen oder Firmen einzubrechen. Der Cyberkriminelle ist ein Mausklick von seinem Opfer entfernt.

Zudem kann im Fall von Online-Betrug der verursachte Schaden weit über dem Wert des gesamten Hab und Gut liegen, das vor Ort gefunden worden wäre. Im Fall von Sextortion kann das Opfer ein schweres psychisches Trauma davontragen, vergleichbar mit demjenigen, das ein Mensch bei physischer Gewalt erlebt. Weiter – ganz im Gegensatz zu den klassischen forensischen Wissenschaften, bei denen sich die Ermittlungen durch die technologische Entwicklung vereinfacht haben (z. B. Spurensuche, Einsatz von DNA-Analysen, 3D-Rekonstruktion von Tatorten) – hat die Entwicklung des IKT-Bereichs die digitale Ermittlung deutlich erschwert.

Routinierte Cyberkriminelle sind inzwischen in der Lage ihre digitalen Spuren zu verändern, zu verfälschen oder zu löschen … und wenn man bedenkt, dass jeder Computer, der in eine cyberkriminelle Handlung verwickelt ist, ein Tatort sein kann … und dass aber auch Computer, die in solche Handlungen verwickelt sind, unschuldigen Personen gehören (deren Computer schlecht geschützt oder infiziert sind und ohne Wissen ihrer Besitzer bei cyberkriminellen Handlungen eingesetzt wurden), versteht man vielleicht die Komplexität der digitalen Ermittlungen. Ja, das Internet hat die Kriminalität grundlegend verändert, vor allem auch, weil die Menschen nicht darauf geschult sind, das Cyber-Pendant der klassischen Formen von kriminellen Handlungen wahrzunehmen.

Welches sind Ihrer Einschätzung nach die wichtigsten Deliktsbereiche im Internet? Und mit Wichtigkeit meinen wir hier: Durch welche internetbasierten Delikte entsteht aus Ihrer Sicht der grösste Schaden hierzulande?

Das ist schwierig zu sagen, da nicht alle Delikte gemeldet werden, weder von Personen noch von Unternehmen, manchmal zögert man zu melden, dass man Opfer eines Online-Betrugs geworden ist, oder einer Erpressung, oder eines Datendiebstahls … aber derzeit scheint Phishing mit dem Ziel, Computer von Personen und Unternehmen mit Ransomware zu infizieren, an erster Stelle zu stehen (90 % der Phishing-Attacken beinhalten Erpressungstrojaner). Europol hat unlängst mitgeteilt, dass Erpressungstrojaner auf europäischer Ebene eine grosse Bedrohung darstellen. Der «Fake President Fraud» nimmt aufgrund der Menge der erschlichenen Gelder ebenfalls einen sehr wichtigen

wk1003mike/Shutterstock.com

«90 % der Phishing-Attacken beinhalten Erpressungstrojaner.»

Platz ein. Andere Arten von Betrügereien, die auf Identitätsdiebstahl oder Social Engineering basieren, sind in den sozialen Medien stark vertreten. Dass der Identitätsdiebstahl kein strafrechtliches Delikt darstellt, erleichtert die Aktivitäten der Cyberkriminellen.

Gibt es Delikte, die vor allem die Schweiz betreffen, und wenn ja, wie erklären Sie sich das?

Die Schweiz wird als reiches Land wahrgenommen, in dem die Bürgerinnen und Bürger über einen hohen Lebensstandard verfügen und deshalb ist sie verglichen mit anderen Ländern ein interessantes Ziel: Angriffe auf kritische Infrastrukturen, DDOS-Angriffe – distributed denial of service – die, wenngleich sie im Ausland ausgeführt werden, Unternehmen und Bewohnerinnen und Bewohner in der Schweiz treffen, da die weltweite Verbreitung von Internetstrukturen und ihre gegenseitigen Verbindungen dies ja erlauben.

Diese Art von Angriffe (DDOS) verfolgen das Ziel, den Zugang zu verschiedenen Dienstleistungen, die vom Internetzugang abhängen, sowohl auf lokaler als auch auf internationaler Ebene zu bremsen oder zu blockieren. Im März 2016 wurden Internetseiten von Schweizer Online-Banken und -Handelsfirmen Ziel eines Angriffs einer Gruppe von Cyberkriminellen mit dem Namen Armada, die es schaffte, den Zugang zu den Dienstleistungen dieser Firmen zu blockieren, nachdem sie sich geweigert hatten, das geforderte Lösegeld zu zahlen. Im September 2016 wurde das «Internet» Ziel des grössten DDOS-Angriffs, den das Netz je erlebt hatte (mirai botnet). Die Besonderheit dieses Angriffs lag darin, dass sich die Cyberkriminellen 400 000 Webcams auf der ganzen Welt bedienten, bei denen die Besitzer das Password nicht personalisiert hatten. Ein ähnlicher Angriff, dessen Folgen auch in der Schweiz zu spüren war, fand im Oktober statt.

Aber das sind nur zwei Beispiele, denen man viele andere anfügen könnte: Angriffe mit Phishing-Versuchen, die Blockade zum Zugang zu digitalen Daten von Personen und Firmen mit Lösegeld-Software, der Diebstahl von Firmendaten (Banken oder andere). Was den Unterschied zwischen den Ländern ausmacht, ist die Menge der Mittel, die jedes Land einsetzt, um die Cyberkriminalität und andere Arten von Angriffen über Netzwerke zu bekämpfen bzw. wie gut das «Bewusstsein» seiner Bürgerinnen und Bürger und Unternehmen ist. Und in diesem Bereich ist die Schweiz im Verzug.

Es gibt gravierende Mängel bei den Mitteln zur Bekämpfung der Cyberkriminalität und das Wissensniveau und die Vorkehrungen von Firmen sowie Einzelpersonen sind nicht ausreichend. Was die notwendigen Mittel betrifft, so ist das vor allem ein politisches Problem, die Schweiz ist ein Opfer ihres Föderalismus zu einem Zeitpunkt bei dem die Welt miteinander verbunden ist und sich nicht um reale, kulturelle und sprachliche Grenzen kümmert … nur Zürich verfügt über einen unabhängigen Ermittlungsdienst gegen Cyberkriminalität (die anderen Kantone haben in den meisten Fällen eine Einheit gegen Computerkriminalität, die andere Polizeidienste unterstützt) und die meisten Beamten sind in den IKT nicht ausgebildet und gleichzeitig wachsen die Aktenstapel. Der Mangel an Bewusstsein und Wissen bei Unternehmen und Einzelpersonen macht die Schweiz zu einem bevorzugten Ziel für Cyberkriminelle.

Der 22. Halbjahresbericht von MELANI, der Melde- und Analysestelle Informationssicherung, der im April 2016 erschienen ist, widmet sich denn auch dem Thema Sicherheitslücken. Der Generaldirektor der französischen Agentur ANSSI formulierte es unlängst wie folgt: *«In den Unternehmen gibt es selbstverständlich einen Verantwortlichen für die Informationssysteme. Er ist unverzichtbar, aber nicht ausreichend. Jeder muss ein Teil der Cybersicherheit sein: der CEO, der Direktor Recht, der Direktor Finanzen … Jeder muss dabei eine Rolle spielen, auch der temporär eingesetzte Mitarbeiter, der in diesen Prozessen häufig vergessen wird, aber oft Zugang zu den Systemen hat.»* Die heutige Situation schwächt die Wirtschaft eines Landes bzw. seine Wettbewerbsfähigkeit und somit sein Wachstum, und das bleibt so, solange die Mentalitäten sich nicht ändern. Zurzeit besteht quasi nichts im Schulunterricht – weder auf der primären, sekundären noch auf der tertiären Stufe unseres Bildungssystems – das es allen erlauben würde, sich die notwendigen Kenntnisse über den digitalen Wandel unserer Gesellschaft anzueignen, um den Wandel zu assimilieren und zu meistern.

www.digital-literacy2020.eu → DLit2.0 Curriculum

Lassen sich in der Schweiz spezifische Opferkategorien erkennen? Gibt es Personen oder Gruppen oder auch Institutionen, die besonders von Internetkriminalität bedroht sind?

Das Verhalten der Cyberkriminellen folgt einer einfachen Logik: Sie versuchen, die Erträge ihrer kriminellen Handlungen zu optimieren und greifen daher die Schwächsten an. In Bezug auf die Cyberkriminalität bedeutet das, dass in erster Linie diejenigen Computer oder Peripheriegeräte angegriffen werden, die am wenigsten gut geschützt sind. Das Profitpotenzial definiert das Ziel. Unternehmen sind daher ein wichtiges Ziel, aber viele kleine Einkünfte durch eine grosse Anzahl von Angriffen auf Individuen generieren ebenfalls einen hohen Gewinn und dies bei einem kleinen Risiko für die Cyberkriminellen (denn jeder betroffene Computer wird für die Polizei und Justiz zu einem neuen Fall). Es ist an dieser Stelle jedoch wichtig zu erwähnen, dass bei der Mehrheit der Betrugsdelikte ein Eingreifen oder eine «Mitarbeit» von Seiten des Opfers notwendig ist, und der Erfolg eines grossen Anteils von Betrugsdelikten auf dem Umstand beruht, dass den Opfern Wissen über und Bewusstsein um die Gefahren fehlt. Einen weiteren Umstand gilt es dabei auch nicht zu vergessen: es gibt gewisse Regierungen (oder Gruppen, die von Regierungen unterstützt werden), die ein cyberkriminelles Verhalten aufweisen und daher gewisse Institutionen oder strategische Tätigkeitsfelder ein Ziel für sie darstellen können. Der Angriff auf die Firma RUAG ist dabei ein gutes Beispiel: die Angreifer verwendeten eine Spyware, um sich in den Server der RUAG einzuschleusen und deren intellektuelles und industrielles Kapital zu plündern. Die Urheber dieses Angriffs – die bis heute formell nicht identifiziert wurden – konnten so während Monaten ungehindert tätig sein, bis man sie schlussendlich entdeckte.

Weerapat Kiatdumrong/123RF

«Cyberkriminelle versuchen, die Erträge ihrer kriminellen Handlungen zu optimieren und greifen daher die Schwächsten an.»

neydt/123RF

«Die Hacktivists sind eine Form von digitalem Schwarzem Block, wie z. B. die Bewegung Anonymous mit ihren gesellschaftspolitischen Forderungen.»

Haben Sie Kenntnisse zur Täterschaft? In der «Offline-Kriminalität» gibt es ja auch spezialisierte Tätergruppen oder bestimmte Motivlagen. Findet sich das auch im Thema Cyberkriminalität und wenn ja, wie sieht es dort aus?

Es ist nicht einfach, eine Bestandesaufnahme der Cyberkriminalität zu erstellen, denn es ist ein polymorpher Bereich, der sich aus vielen grauen Nuancen zusammensetzt … z. B. gibt es nicht die Hacker und den Rest der Welt … viele Strömungen sind präsent und es ist dabei wichtig, diese zu definieren und zu kategorisieren: es gibt folgende Gruppen: die **«Black Hats»** (kriminelles Verhalten); die **«White Hats»** (ethisches Verhalten, ethische Hacker, nützlich für die Gesellschaft, sie lassen die Sicherheitslücken schliessen); die **«Grey Hats»** (von beiden etwas): die **«state sponsored hackers»** (kriminelles Verhalten – inoffiziell – von einem Staat unterstützt, oder von Nationalisten, die de facto ihr Land mit Angriffen unterstützen); die **«Hacktivists»** (eine Form von digitalem Schwarzem Block, wie z. B. die Bewegung **Anonymous** mit ihren gesellschaftspolitischen Forderungen. Im Grund sind sie keine Kriminellen, aber die Art ihres Verhaltens kann es sein.); die **«Cyberkriminellen»** (Ausweitung und Entwicklung von klassischen kriminellen Handlungen in den Cyberspace); die **«Script kiddies»** (meistens Jugendliche oder Personen, die von anderen entwickelte Software, die über ein gewisses Angriffspotenzial verfügt, verwenden, weil sie selbst nicht über ausreichend Expertise verfügen, um solche Programme zu entwickeln); die **«Cyber-Söldner»,** die ihre Informatikkenntnisse zu Geld machen. (Die Affäre Giroud ist dafür ein gutes Beispiel. Der Walliser Weinhändler wurde angeklagt, einen Cyber-Söldner beauftragt zu haben, ihn beschuldigende Dokumente auf den Computern von zwei Journalisten zu löschen.)

Zusammenfassend kann man sagen, dass diese kleine Welt einerseits die Vielfalt und andererseits die Komplexität der Akteure in den digitalen Welten widerspiegelt. Diese Komplexität wird durch den Umstand verstärkt, dass sich Cyberkriminelle wie Unternehmer und gewisse Unternehmer (oder Regierungen) sich wie Cyberkriminelle verhalten. Man beobachtet aber auch sogenannte «Teilzeit-Cyberkriminelle», die ab und zu dunklen Machenschaften im Netz nachgehen, einfach weil sie die Risiken im Vergleich zu den potenziellen Einnahmen als gering einschätzen, aber im Alltag bei einem Unternehmen angestellt sind (théorie des opportunités en criminologie, Walsh, 1986). Dann gibt es auch noch diejenigen, die nach Sicherheitslücken suchen, um sie danach zu verkaufen – unter anderem auch im Darknet (dem Graumarkt der Cyberkriminalität). Sie begehen damit keine kriminelle Tat, liefern aber die «Waffen und die Munition» bzw. die notwendigen Ressourcen, deren sich die Cyberkriminellen dann bedienen. Es ist ein sehr lukrativer Markt mit wenig Risiken … gewisse Sicherheitslücken lassen sich für mehrere Hunderttausend Franken verkaufen. Der Graumarkt der Sicherheitslücken beliefert aber nicht nur Cyberkriminelle, sondern auch Unternehmen, Regierungen

und deren Nachrichtendienste. Gewisse Regierungen haben dafür einen besonderen Budgetposten.

Im Jahr 2012 versuchte Michael McGuire des John Grieve Center for Policing and Safety in London (GB) mit der Studie «Organised Crime in the Digital Age», ein Bild der potenziellen Beziehung zwischen dem organisierten Verbrechen und der Cyberkriminalität zu zeichnen. Laut dieser Studie verfügen 80 % der cyberkriminellen Gruppen über organisierte Strukturen, ohne dass diese Gruppierungen zwingend aus dem klassischen organisierten Verbrechen stammen müssen. 43 % der Mitglieder dieser cyberkriminellen Organisationen sind älter als 35 Jahre und 29 % sind jünger als 25 Jahre. Die Hälfte der Gruppen besteht aus sechs Mitgliedern oder mehr, ein Viertel besteht aus 11 oder mehr Mitgliedern. 25 % der aktiven Gruppen waren weniger als sechs Monate aktiv.

http://www.cybercrimejournal.com/broadhurstetalijcc2014vol8issue1.pdf

Sie sind auch in der Bekämpfung von Wirtschaftskriminalität ausgebildet: Können Sie uns etwas zur Bekämpfung der Wirtschaftskriminalität im Netz sagen? Wo liegen die Schwerpunkte bzw. wo sollten sie liegen? Und welche Mittel stehen der Strafverfolgung zur Verfügung?

Mit der starken Zunahme des Einsatzes der IKT, der zunehmenden Entmaterialisierung der Dienstleistungen sowie dem Aufkommen des Internets der Dinge sehen wir eine Zunahme der Wirtschaftskriminalität in der digitalen Welt. Immer mehr digitale Dienste und Objekte unseres Alltags sind miteinander verbunden und tauschen Daten untereinander aus. Ein am Internet angeschlossener Kühlschrank birgt noch nicht zu viele Probleme, aber eine Insulinpumpe, ein Herzschrittmacher, ein Auto oder das Schliesssystem unserer Wohnung usw. schon. Dabei ist es ein Problem für die Polizei und die Justiz an die notwendigen Ressourcen zu gelangen, die es ihnen ermöglichen würde, auf die grosse Zahl von Fällen adäquat zu reagieren. Und die Fälle, die in der Schweiz stattfinden, machen vor unseren Grenzen nicht Halt. Polizei und Justiz brauchen deshalb meist europäische oder weltweite Unterstützung und diese bedarf Rechtshilfebegehren und das braucht Zeit – und diese Zeit kommt den Cyberkriminellen zugute. Es gibt wohl Europaratskonventionen zur Cyberkriminalität, die im Jahr 2012 auch in der Schweiz gültig wurden, aber nicht alle europäischen Länder haben sie unterzeichnet und diese Schwachstellen werden von den Cyberkriminellen rege ausgenutzt. Cyberkriminelle engagieren etwa Rechtsexperten, um zu evaluieren, welches Land sie am besten als Basis für ihre Angriffe wählen sollen.

Was würden Sie einem Anwalt, der im Bereich Strategien für den Datenschutz bei Cyberkriminalität spezialisiert ist, empfehlen, wenn es um Strafverfolgungsmassnahmen in der Schweiz geht?

Auf der Ebene Strafrecht müssen grundsätzliche Überlegungen angestellt werden und sie dürfen nicht nur der Justiz und der Politik überlassen werden. Im Bereich IKT hat das Milizsystem seine Grenzen erreicht. Es ist sehr wichtig, dass Professionelle, die in ihrem Alltag gegen Cyberkriminalität kämpfen – sowohl im öffentlichen als auch im privaten Sektor – diejenigen Probleme zur Sprache bringen können, mit denen sie konfrontiert sind. Die mangelnden Kenntnisse der Politikerinnen und Politiker über die Informationsgesellschaft (die spezialisierten Kommissionen inbegriffen) wirken sich extrem nachteilig auf das Verständnis für die Probleme aus, die sich bei der Bekämpfung der Cyberkriminalität stellen. Anfang 2013 wurden der Rechtsanwalt François Charlet und ich von einer politischen Partei eingeladen, unsere Überlegungen zu den Schwierigkeiten im Zusammenhang mit den IKT zu präsentieren. Nach diesem Treffen wurde das Thema Identitätsdiebstahl und -missbrauch zu einem prioritären Dossier der Partei erklärt … seitdem hat sich aber, wir sind im Jahr 2016, allein die Zahl der Opfer weiterentwickelt. Das gleiche gilt für den Verlust von Daten. Die Europäische Kommission hat die NIS-Richtlinien (The Directive on security of network and information systems) erarbeitet, die 2018 in Kraft treten sollen.

https://ec.europa.eu/digital-single-market/en/network-and-information-security-nis-directive

Sie enthalten unter anderem auch eine Meldepflicht im Fall von Piraterie oder Einbruch in die IKT bei Infrastrukturen, die als kritisch eingestuft sind, sowie

rangizzz/123RF

«Polizei und Justiz brauchen meist europäische oder weltweite Unterstützung und diese bedarf Rechtshilfebegehren und das braucht Zeit – und diese Zeit kommt den Cyberkriminellen zugute.»

die Verpflichtung für Unternehmen, in denen Daten verschwunden sind, dies den zuständigen Behörden (auf nationaler Ebene) und den betroffenen Personen innert drei Tagen zu melden. Sie verpflichtet die betroffenen Akteure zudem, notwendige Optimierungsmassnahmen zu ergreifen, um eine wirksame Sicherheit zu gewährleisten. Die Schweiz – die Einige auch als zukünftigen «digitalen Safe der Welt» sehen – muss baldmöglichst solche Richtlinien erarbeiten.

Auf der Ebene von Personen sind sowohl die Juristen als auch die Behördenvertreterinnen und -vertreter in der Schweiz im Verzug und scheinen mit den Realitäten unserer (vernetzten) Gesellschaft nicht genügend vertraut zu sein. Ich habe Fälle von Sextorsion und revenge porn (Verbreiten von intimem Bildmaterial sexuellen Charakters des Partners/der Partnerin ohne dessen/deren Einverständnis) behandelt, bei denen, nach Schweizer Recht, das Opfer, je nach Alter, potenziell für die Herstellung und Verbreitung von pornografischen Inhalten als schuldig befunden werden könnte. Nicht genug, dass man den Status als Opfer nicht anerkannt, noch dazu riskiert der Täter nicht viel: im Jahr 2013 wurde im Kanton Waadt ein Mann für die Verbreitung von intimen Videos seiner Ex-Freundin auf einer Porno-Website für schuldig befunden – das Urteil lautete auf eine Geldstrafe von nur 50 Tagesansätzen auf Bewährung (Frauen sind zu 80 % Opfer solcher Handlungen). Das Gleiche gilt wenn eine Frau vergewaltigt wird und die Vergewaltiger ihre Tat filmen und bei WhatsApp verbreiten – wie es auch schon passiert ist – oder dies im Internet tun, so werden die Vergewaltiger vom Richter (eventuell) der Vergewaltigung für schuldig befunden. Aber der Richter wird dabei den Umstand nicht berücksichtigen, dass es sich bei einer Vergewaltigung, mit der Absicht sie zu filmen und zu verbreiten – im rechtlichen Sinn – um einen Akt der Grausamkeit handelt, bei dem die Täter dem Opfer also aus gefühlloser, unbarmherziger Gesinnung besondere körperliche oder seelische oder seelisch-körperliche Qualen zufügen.

Das Urteil sollte die rechtliche Verpflichtung enthalten, die inkriminierten Inhalte aus dem Internet zu nehmen und sollte dies nicht geschehen, sollte mit weiteren rechtliche Sanktionen gedroht werden können. Mit anderen Worten: damit sich das Gesetz weiterentwickelt, müssen sich die Mentalitäten verändern. Es ist wichtig, dass die betroffenen Organisationen ein Bewusstsein für das Opfer und die potenziellen Traumata entwickeln, die aus den Aggressionen im Internet resultieren können bzw. für den potenziellen posttraumatischen Stress, den das Wiederauftauchen von beleidigendem Bildmaterial auslösen kann. Diese Veränderung der Mentalität ist auch notwendig, damit die Entscheidungsträger die Arbeit der Polizei und deren Schwierigkeiten bei ihrer Arbeit im Internet besser verstehen. Als positives Beispiel nenne ich hier die verdeckte Ermittlung, die es der Polizei im Rahmen ihrer Ermittlungen ermöglicht, eine falsche Identität zu verwenden. Das Gesetz trat 2005 in Kraft.[1]

Wie wird sich die Internetkriminalität verändern und wodurch? Wird es neue Delikte geben?

Der Kriminologe Michael McGuire definiert die Cyberkriminalität als die vierte Ära der Kriminalität. Ich kann es wie folgt sagen: Mehr Verbrechen – weniger Mittel um sie zu bekämpfen. Man muss die Zunahme der Cyberkriminalität nicht als Schicksal akzeptieren. Aber es müssen die Mittel, die es braucht, um sie zu bekämpfen, zur Verfügung stehen, sei dies auf finanzieller, rechtlicher oder polizeilicher Ebene. Im Zentrum dieses Krieges gegen die Cyberkriminalität steht immer das Wissen. Schlussendlich verwenden die Cyberkriminellen die gleichen Technologien wie wir. Ein grosser Teil der Cyberangriffe und Betrugsversuche in Internet basieren auf dem Unwissen der Anwenderinnen und Anwender. Wenn wir das Phishing als Beispiel nehmen wollen: das Internet gibt es etwa seit 25 Jahren und man hat es bis anhin nicht verstanden, den Anwenderinnen und Anwendern beizubringen, einen Weblink (URL) richtig zu lesen – auf ihrer Manipulation basiert der Betrug im Internet.

Welche Rolle spielt das Darknet in der Internetkriminalität? Hat die Polizei überhaupt eine Chance, Delikte im Darknet aufzuspüren oder bräuchte es Gesetzesänderungen?

Das Problem Darknet ist nicht nur ein rein rechtliches Problem. Die Werkzeuge, die hier die Anonymität ermöglichen, sind die gleichen wie diejenigen, die von Menschenrechtsaktivistinnen und -aktivisten oder von Journalistinnen und Journalisten in undemokratischen Ländern verwendet werden, um von Übergriffen auf die persönlichen Freiheiten oder von korrupten Regierungen zu berichten. Diese Werkzeuge retten auch Leben.

Die Lösung besteht also nicht darin, diese Technologien zu schwächen, sondern darin, die Expertise sowie die Zusammenarbeit und den Informations- und Erfahrungsaustausch zwischen den verschiedenen Polizeiorganen und der Justiz zu verbessern, und das sowohl auf nationaler als auch auf internationaler Ebene. Zudem zeigt sich, dass das Darknet nicht undurchdringlich ist: im Jahr 2013 gelang es dem FBI «Silk Road» zu schliessen, einen der grössten illegalen Handelsplätze im Darknet. Weiter gelang es dem FBI von Anfang an, sich in Silk Road 2.0 einzuschleichen und es im darauffolgenden Jahr zu schliessen. Zurzeit besteht bereits eine neue Version der Site, die floriert, vor allem beim Verkauf von Drogen. Aber wo besteht da der Unterschied zur realen Welt? Auch da schafft man es nicht, den Drogenhandel zu

1 https://www.bj.admin.ch/bj/de/home/sicherheit/gesetzgebung/archiv/verdeckte-ermittlungen.html Bundesgesetz über die verdeckte Ermittlung

scanrail/123RF

«Die Polizei ist mit adäquatem Wissen und passenden Mitteln sehr wohl in der Lage, auf allen technologischen Ebenen gegen die Cyberkriminalität vorzugehen.»

unterbinden. Was ich damit sagen will ist, dass die Polizei mit adäquatem Wissen und passenden Mitteln sehr wohl in der Lage ist, auf allen technologischen Ebenen gegen die Cyberkriminalität vorzugehen.

Was sind wichtige Präventionstipps gegen Internetkriminalität?

Auch auf die Gefahr hin mich zu wiederholen: der Wissensstand der Anwenderinnen und Anwender, sei es nun eine Einzelperson oder eine Firma, muss deutlich besser werden. Sonst kann man gar nichts erreichen. Der Staat sollte diese Wissensvermittlung mit dem adäquaten Einsatz von Ressourcen ermöglichen. Entweder über das öffentliche Bildungswesen, über Unternehmen, oder warum auch nicht über die Armee (ich könnte mir eine Schulung während der Rekrutenschule gut vorstellen). In Frankreich z. B. haben das Nationale Institut für Sicherheit und Justiz (INHESJ) und die Interministerielle Delegation für Wirtschaftinformation (D2IE) in einer gemeinsamen Erklärung verlauten lassen, dass sie planen, «Spezialisten in Wirtschaftssicherheit» auszubilden, die aus der Wirtschaft kommen. Ziele dieses Vorgehens sind die Erarbeitung einer gemeinsamen Haltung und Botschaft zu Wirtschaftssicherheitsfragen und die gemeinsame Förderung der bestehenden sowie der zu entwickelnden Mittel. Meines Erachtens ist es ebenso eine Aufgabe des Staates, Gefahren zu identifizieren, die Unternehmen und Privatpersonen nicht in der Lage zu erkennen sind. Es sollten auf Regierungsebene Strukturen geschaffen werden, mit denen man unter Verwendung von Mitteln aus dem Privatsektor, in der Lage ist, nach zukünftigen Gefahren zu suchen und Instrumente, die in strategischen Infrastrukturen des Landes verwendet werden, zu evaluieren (Hardware, Software, Firmware). Die Zukunft der wirtschaftlichen Sicherheit in der Schweiz, das Innovationspotenzial und das Wachstum stehen auf dem Spiel. Auf rechtlicher Ebene sollten Unternehmen, die ihre Daten nicht ausreichend schützen, sanktioniert werden können.

Die Anwenderinnen und Anwender hingegen sind verantwortlich dafür, die Geräte, die sie verwenden, zu verstehen. Ein Grossteil der Bevölkerung ist damit einverstanden, sich eigenverantwortlich über verordnete Medikamente, die Zusammensetzung von Lebensmitteln, die man konsumiert, oder über das Funktionieren eines Autos zu informieren sowie «neue Regeln» in der realen Welt zu akzeptieren.

Das sollte in der Welt der Informations- und Kommunikationstechnologien nicht anders sein. Sie sind die Basis der digitalen Veränderung unserer Gesellschaft, und die digitale Welt ist davon nur die dematerialisierte Realität … aber es ist trotzdem die Gesellschaft, unsere Gesellschaft, in der wir leben und kein virtueller Raum losgelöst vom hier. Oder wie es der französische Philosoph Edgar Morin sagte: «Um in einer komplexen Gesellschaft zu leben, muss man sich komplexes Denken aneignen können.» Ich erlaube mir, seine Gedanken etwas umzuformulieren, im Sinne von: «Sich Zeit nehmen, um zu lernen mit seiner Zeit zu leben, damit man nicht weltfremd wird.»

Wer bekämpft die Internetkriminalität und wer schützt die digitalen Strukturen in der Schweiz?

Die Strategie des Bundesrates für eine digitale Schweiz und ihre Auswirkung auf die Sicherheit der Bevölkerung

Mit der im April 2016 verabschiedeten Strategie «Digitale Schweiz» will der Bundesrat dazu beitragen, dass die Schweiz mehr von der zunehmenden Digitalisierung profitiert. Mit Blick auf eine informierte und demokratische Gesellschaft ist es zudem von zentraler Bedeutung, dass die Einwohnerinnen und Einwohner der Schweiz die modernen Informations- und Kommunikationstechnologien in ihrem täglichen Leben kompetent und sicher nutzen können.

Im Rahmen der Strategie sollen u. a. folgende sicherheitsrelevante Massnahmen umgesetzt werden:

- Durchführen der Vernehmlassung zur Revision des Fernmeldegesetzes (FMG), das dem Bund Möglichkeiten zum Schutz Jugendlicher vor den Gefahren der Fernmeldedienste überlässt. So sollen Anbieter von Internetzugängen verpflichtet werden können, ihre Kundschaft über Jugendschutzmassnahmen zu beraten und kinderpornografische Inhalte zu sperren (Umsetzung bis Ende 2016).
- Abklären der Möglichkeiten zum Schutz der Privatsphäre von Nutzerinnen und Nutzer der digitalen Medien, insbesondere von Kindern und Jugendlichen, im Rahmen der Revision des Datenschutzgesetzes (Umsetzung bis Ende 2016).
- Verstärken des Jugendmedienschutzes vor ungeeigneten Inhalten mittels Alterskennzeichnung und Abgabebeschränkungen für Videos und Games mit einem neuen Gesetz (Umsetzung bis Ende 2017).
- Beurteilen der Entwicklung von Datensicherheit und Datenbearbeitung (Big Data), Beurteilen der Folgen für die Gesellschaft und Überprüfung des bestehenden Rechtsrahmens (Umsetzung bis Mitte 2018).

Mehr Informationen unter:
www.bakom.admin.ch → Digitale Schweiz und Internet → Strategie «Digitale Schweiz»

Die Koordinationsstelle zur Bekämpfung der Internetkriminalität (KOBIK)

KOBIK ist bei der Bundeskriminalpolizei (BKP) angegliedert, einer Hauptabteilung des Bundesamtes für Polizei (fedpol).

KOBIK betreibt verdachtsunabhängige Recherchen im Internet. Nach der Analyse der erstellten Dossiers und Fälle werden diese – entsprechend ihrer strafrechtlichen Relevanz – an die zuständigen Strafverfolgungsbehörden im In- und Ausland weitergeleitet. Als strafrechtlich relevant gelten Inhalte im Internet, die eines der nachstehenden Merkmale aufweisen (nicht abschliessend):

- harte Pornografie (sexuelle Handlungen mit Kindern oder mit Tieren oder gewalttätige sexuelle Handlungen)
- legale Pornografie, die auch von Minderjährigen konsumiert werden kann, wenn weder ein Kinderschutz noch eine Alterskontrolle angeboten wird
- Gewaltdarstellung
- Rassismus, Extremismus
- Ehrverletzungen, Drohungen
- Betrug, Wirtschaftsverbrechen
- unbefugtes Eindringen in Computersysteme
- Verbreitung von Computerviren, Datenbeschädigung

Für Personen, die verdächtige Internetinhalte melden möchten, steht auf der Internetseite www.cybercrime.ch ein Formular zur Verfügung.

KOBIK steht als Kompetenzzentrum der Öffentlichkeit, den Behörden und Internet-Service-Providern für rechtliche, technische und kriminalistische Fragen zur Internetkriminalität zur Verfügung. KOBIK ist als nationale Koordinationsstelle zur Bekämpfung der Internetkriminalität auch Ansprechpartner für ausländische Stellen, die analoge Aufgaben wahrnehmen.

Mehr Informationen unter:
www.cybercrime.admin.ch

Die Melde- und Analysestelle Informationssicherung (MELANI)

MELANI ist ein Kooperationsmodell zwischen dem Eidgenössischen Finanzdepartement (EFD), vertreten durch das Informatiksteuerungsorgan des Bundes (ISB), und dem Eidgenössischen Departement für Verteidigung, Bevölkerungsschutz und Sport (VBS), vertreten durch den Nachrichtendienst des Bundes (NDB).

MELANI steht zwei Kundenbereichen zur Verfügung: Der **Offene Kundenkreis,** an den sich MELANI richtet, umfasst private Computer- und Internetbenutzer sowie kleinere und mittlere Unternehmen (KMU) in der Schweiz.
Zu ihrem Schutz bietet MELANI:

- Informationen über Gefahren und Massnahmen im Umgang mit

modernen Informations- und Kommunikationstechnologien (z. B. Internet, E-Banking).
- Berichte, welche die wichtigsten Tendenzen und Entwicklungen rund um Vorfälle und Geschehnisse in den Informations- und Kommunikationstechnologien (IKT) erläutern.
- Ein Meldeformular um Vorfälle, von denen Anwenderinnen und Anwender persönlich betroffen sind, zu melden.

Der **Geschlossene Kundenkreis** umfasst ausgewählte Betreiber von kritischen Infrastrukturen (z. B. Energieversorger, Telekommunikationsunternehmen, Banken usw.) auf Landesebene. Hier ist es die Aufgabe von MELANI, diese Infrastrukturen zu schützen, insbesondere dort, wo diese vom Funktionieren der Informations- und Kommunikationsinfrastrukturen abhängen.

Mehr Informationen unter:
www.melani.admin.ch

Der Ende Oktober erschienene Halbjahresbericht «Informationssicherung – Lage in der Schweiz und International» zeigt die wichtigsten Cybervorfälle der ersten Jahreshälfte sowohl national als auch international auf. Der Bericht widmet sich im Schwerpunktthema den vermehrten Angriffen durch Cybererpressung.

www.melani.admin.ch → Dokumentation → Berichte → Lageberichte → Halbjahresbericht 2016/1

Häufige Internetdeliktformen

Aufgrund ihrer langjährigen Erfahrung mit Delikten im Internet ist die SKP sehr häufig die erste Ansprechpartnerin für Bürgerinnen und Bürger. Die SKP nimmt aber auch die Erstberatung und Triage von Opfern aus Fällen im Bereich der digitalen Medien wahr, z. B., ob eine Anzeige sinnvoll ist oder wer Ansprechpartner bei der Polizei ist. Im Gespräch mit den Opfern erhält sie zudem wertvolle Hinweise zu den Täterstrategien, die es ihr dann wiederum ermöglichen, die Präventionsbotschaften zu den verschiedenen Deliktformen zu aktualisieren.

In diesem Beitrag beschreibt die SKP diejenigen Delikte, die von der Bevölkerung am häufigsten zur Sprache gebracht werden. Sei es, weil die Anrufenden selber Opfer wurden oder sie vermuten, dass ein Angehöriger, eine Freundin oder ein Freund Opfer dieser Delikte werden könnte.

Wenn Lust und Liebe zu Last und Leid führen

Dass Gauner im Netz mit allen möglichen Tricks und Maschen betrügen, ist inzwischen hinlänglich bekannt. Damit eine Person zum Opfer wird, muss sie logischerweise auf die Lügen hereinfallen, und das geht sehr viel einfacher, wenn die grundsätzliche Bereitschaft vorhanden ist, dem Angebot Glauben zu schenken. Diese Bereitschaft entsteht durch einen subjektiven Mangel: einen Mangel an Geld, an Prestige oder eben auch einen Mangel an körperlicher oder seelischer Zuwendung.

Die folgenden zwei Betrugs- bzw. Erpressungsformen zielen genau auf diese Schwächen und haben demzufolge Menschen im Visier, die auf der Suche nach menschlicher Wärme oder körperlicher Lust sind, auch wenn sie sich im Einzelnen sehr unterschiedlich präsentieren.

Romance Scam

Die Liebeslüge oder der Digitale Heiratsschwindler

Unter den Fachbegriffen «Romance Scam» oder «Love Scam» versteht man eine Form von Internetbetrug, der auf Menschen mit einem starken Partnerwunsch abzielt. Diese Betrugsform ist insofern besonders hinterhältig, als dass sie nicht nur leere Konten, sondern auch gebrochene Herzen hinterlässt. Wie läuft das genau?

Der Modus Operandi

Betrüger und Betrügerinnen geben sich unter falschen Identitäten in Partnerbörsen und in sozialen Netzwerken als verliebte Verehrerinnen und Verehrer aus. Sie umwerben die Opfer mit Komplimenten und Liebesschwüren und versuchen anschliessend, ihnen mit rührseligen Geschichten Geld aus der Tasche zu ziehen. So kommt es beispielsweise vor, dass der selbsternannte kanadische Ingenieur Bob Tyler[1], gutaussehend und gut situiert, auf einer Partnersuchplattform Frau Susanne Meier[2] aus N. anschreibt und ihr nach kurzer Zeit sehr eindringlich und

1 fiktiver Name
2 fiktiver Name

stokkete/123RF

Romance Scam: Diese Betrugsform ist insofern besonders hinterhältig, als dass sie nicht nur leere Konten, sondern auch gebrochene Herzen hinterlässt.

blumig vermittelt, dass genau sie die Frau seiner Träume sei. Frau Meier ist nicht sehr misstrauisch im Internet und weiss vielleicht nicht, wie einfach man ganze Profile von A bis Z fälschen kann und dass E-Mail-Adressen oder Telefonnummern keine sicheren Hinweise mehr auf die Herkunftsländer geben. Frau Meier sehnt sich zudem nach einer Partnerschaft und hat schon lange keine romantischen Worte mehr gehört. Endlich hat auch sie einmal Glück und trifft auf die grosse Liebe! Love-Scammer sind Meister im Umwerben, Umschmeicheln und Umgarnen, und je länger Frau Meier mit Herrn Tyler chattet oder auch telefoniert, desto überzeugter ist sie von der Ernsthaftigkeit der Werbung. Warum sollte sich denn sonst jemand so viel Mühe geben? Liebe macht nicht nur blind, das wissen wir alle auch aus eigenen Erfahrungen. Beim Love-Scam kommt dazu, dass die spezifischen Täuschungs- und Fälschungsmechanismen im Netz nicht bekannt sind und deshalb die Lüge noch schwerer als solche erkannt wird.

Wenn der Betrüger dann sicher ist, dass er eine genügend starke emotionale Abhängigkeit erreicht hat und ein persönliches Treffen konkret angebahnt worden ist, folgen Schilderungen von Unfällen, Krankheitsfällen, Behördenproblemen oder familiären sowie geschäftlichen Notfällen. So ist Herr Tyler zum Beispiel angeblich auf dem Weg in die Schweiz, musste aber geschäftlich über Dubai reisen. Dort kann ein Geschäft nur erfolgreich abgeschlossen werden, wenn sofort eine gewisse Summe vorgeschossen wird, wobei Herr Tyler aus unterschiedlichsten Gründen keinen Zugriff auf seine eigenen Finanzen hat und deshalb Frau Meier doch so nett sein müsste, so rasch als möglich die Summe zu überweisen, damit die Reise in die Schweiz endlich angetreten werden kann. Mit solchen Geschichten ergaunern sich Romance-Scammer nicht selten Hunderttausende von Franken, bis das verliebte Opfer realisiert, dass nicht sein Herz, sondern seine Brieftasche Ziel der Werbung war.

Da die E-Mails, Telefonnummern und Profile allesamt gefälscht resp. anonymisiert sind, die Zahlungen über Geldtransferdienste wie «Western Union» oder «Moneygram» erfolgen und somit auch der Geldfluss nicht nachverfolgt werden kann, ist das Geld verloren. Zusätzlich wurde das Vertrauen der Betroffenen erschüttert, und die Scham ist gross.

Der Modus Operandi «für Fortgeschrittene»

Und wie wenn das nicht genug wäre, geht der Lug und Trug noch weiter. Nicht oder nicht mehr zahlungswillige Opfer werden mit gefälschten Schreiben von angeblichen Polizei- und Justizbehörden massiv unter Druck gesetzt und mit der Aussicht, den Betrüger dingfest zu machen, wiederum zu Vorschusszahlungen überredet: Ein spezialisierter Interpol-Ermittler soll Herrn Tyler entlarvt haben und somit wisse Interpol, dass Frau Meier Opfer wurde. Damit das Geld zurückerstattet werden könne, müsse Frau Meier diese und jene Zahlungen beim Zoll oder bei der Justiz in Dubai veranlassen, um wieder an ihr Geld zu kommen. So kann es passieren, dass die Betroffenen doppelt betrogen werden und anstatt Hilfe zu bekommen, noch mehr Schulden am Hals haben. Die Betrüger sind kreativ, innovativ, hartnäckig, geduldig, mit allen Wassern gewaschen und sehr bewandert im Umgang mit den digitalen Medien. Und wie berichtet, kann diese kriminelle Tätigkeit sehr lohnenswert sein.

Präventionsmassnahmen gegen Romance Scam

Vertrauen ist gut, Misstrauen ist manchmal besser. Gerade weil die Strafverfolgung bei diesem Internetbetrug kaum eine Chance hat, die Betrüger zu ermitteln, ist die Prävention umso wichtiger. Informierte Partnersuchende erkennen die Masche relativ gut, gerade weil sie so standardisiert abläuft. Deshalb ist es wichtig, diese Betrugsform bekannt zu machen. Und ein Tipp hilft garantiert:

Zahlen Sie niemals Geld an Menschen, die sie nicht persönlich – d. h. aus dem Offline-Leben – kennen, mag die Geschichte dahinter noch so herzerweichend sein!

Sextortion oder Erpressung über kompromittierendes Bild- und Videomaterial

Das Prickeln vor dem bösen Erwachen

Vielleicht ist es ein Cliché, dass Männer eher über körperliche Reize, als mit romantischen Worten im alten Spiel zwischen den Geschlechtern «geködert» werden. Tatsache ist, dass beim

Love-Scam oft Frauen Opfer werden (aber nicht nur!) und dass bei der folgenden Masche eher Männer Zielpersonen sind. «Sextortion», eine Wortschöpfung aus «Sex» und «Extortion» (engl. für Erpressung), ist selbstredend, denn genau darum geht es: Menschen, meist Männer, werden in sozialen Netzwerken (Facebook, WhatsApp etc.) von «sexy Ladies» sehr offensiv angemacht. Nach einem kurzen Chat folgt bald die Einladung, in einen Videochat wie z. B. Skype zu wechseln. Dort wird es rasch prickelnder und offenherziger. Die Damen bieten erotische Shows und fordern das Gegenüber auf, beim Cybersex mitzumachen. Zu zweit mache es doch viel mehr Spass! Aus Spass wird aber sehr schnell Ernst! Sobald die Damen über kompromittierendes Videomaterial verfügen, zeigt sich unmittelbar das wahre Motiv hinter der Anmache. Die Betrügerinnen verlangen Geld und drohen, andernfalls die Aufnahmen auf YouTube zu veröffentlichen oder direkt an die Facebook-Freundesliste der Betroffenen zu schicken.

loganban/123RF

Sextortion: Zielpersonen sind meistens Männer.

Zahlen schützt nicht!

Natürlich ist die Scham teils riesig und die Opfer trauen sich nicht, mit anderen über die Erpressung zu sprechen. Aus Angst, dass die Familie, die Freunde oder die Berufskolleginnen und -kollegen intimes Filmmaterial zu sehen bekommen, zahlen einige die geforderte Geldsumme von in der Regel ein paar hundert Euros, Dollars oder auch Schweizer Franken.

Wiederum ist es wichtig, dass im Vorfeld gut informiert wird, was auch hier nicht schwierig ist: Tun Sie es nicht! Kein Cybersex im Videochat mit Unbekannten! Alles, was im Netz abgerufen werden kann, hat Missbrauchspotenzial und intimes Material eignet sich nun einmal sehr gut für Missbrauch.

Das Bonmot «Think before you post» wirkt je nach Grad der Erregung leider nicht mehr. Wenn jemand also einen schwachen Moment hatte und sich der Illusion hingab, die «heisse Lady» aus dem Webcam-Land wäre wirklich verrückt nach ihm und nicht nach seinem Geld, sollte Folgendes beachtet werden:

- Ruhe bewahren, sofort jeglichen Kontakt abbrechen: die Adresse blockieren und/oder den Fake-Account der Erpresserinnen dem Seitenbetreiber melden.
- Auf keinen Fall auf die Forderungen eingehen und kein Geld überweisen! Das Bezahlen schützt nicht vor einer Veröffentlichung. Im Gegenteil, die Erpresserinnen werden oft noch dreister und fordern mehr Geld, wenn sie wissen, dass jemand erpressbar ist.
- Betroffene können für ihren Namen einen «Google Alert» einrichten. Auf diese Weise werden sie über neue Videos, Fotos oder andere Inhalte, die mit ihrem Namen versehen sind, informiert.
- Falls Fotos und/oder Videos im Internet auftauchen (und das ist bei Weitem nicht immer der Fall) sollten die Seitenbetreiber informiert werden – soziale Netzwerke wie z. B. Facebook löschen sexualisierte Inhalte in der Regel rasch.

Und auch wenn es bei diesem Delikt für die Polizei ebenfalls kaum möglich ist, an die Hintermänner und -frauen zu gelangen, da aus der Anonymität heraus agiert wird, sollten diese Internetdelikte angezeigt werden. Nur so erhält die Polizei Informationen zum Ausmass des Deliktfeldes, kann Zusammenhänge herstellen und allenfalls Ermittlungsmöglichkeiten finden.

Dazu müssen relevante Beweismittel, welche die Erpressung bzw. den Betrug belegen, gesichert werden: Screenshots der betrügerischen Accounts, das Chatprotokoll und/oder der E-Mail-Verkehr. Anzeige kann bei jeder Kantonspolizei erstattet werden. Erpressung und Betrug sind Offizialdelikte und werden somit von Amts wegen verfolgt.

Und ein wichtiger Punkt zum Schluss: Keine Angst vor Peinlichkeiten: Die Polizei ahndet Verbrechen, keine menschlichen Schwächen!

Vorschussbetrug

Was versteht man unter «Vorschussbetrug»?

Die Deliktform Vorschussbetrug kennt man seit über 30 Jahren. Ein Betrüger versucht, für ein Produkt oder eine Dienstleistung vom (potenziell) Geschädigten Geld im Voraus zu erhalten, und wird dann weder das Produkt liefern noch die Dienstleistung erbringen. Bekannt geworden ist der Vorschussbetrug mit angeblichen Lotteriegewinnen («Sie haben in Spanien 2 Mio. Euros gewonnen, holen Sie sich Ihren Gewinn!») oder vorgetäuschten Erbschaften («Ein Onkel mit einem grossen Vermögen, den Sie persönlich nicht kennen, ist in Namibia gestorben. Wir senden Ihnen Ihre Erbschaft.»), die brieflich, per Fax oder per E-Mail bei den Geschädigten eingetroffen sind. Heute wird Vorschussbetrug fast nur noch über E-Mails oder Webseiten betrieben.

In welcher Form wird Vorschussbetrug häufig festgestellt?

Die SKP hat einen breiten Überblick über die häufigsten Vorschussbetrugsarten.

Meldungen erhält die SKP von Medien, Konsumentenorganisationen sowie Einwohnerinnen und Einwohnern, die entweder direkt von einem Betrugsfall betroffen sind oder die sich für jemand anderen informieren. Als Opfer stark betroffen scheinen ältere Menschen, die sich in den digitalen Medien nicht so gut auskennen und immer noch glauben, das in den Betrug investierte Geld eines Tages zurückzuerhalten. Häufig erkundigen sich Familienmitglieder bei der SKP, wie sie eine ältere Person davon überzeugen können, dass sie Opfer eines Betruges geworden ist.

Die SKP gibt meist in vier Fällen von Vorschussbetrug Auskunft:

1. Lotterie-Vorschussbetrug

zentilia/123RF

Die Betrüger informieren die Opfer meist per E-Mail über den Gewinn des Hauptpreises einer Lotterie im Ausland, sehr beliebt ist im Moment die «Loteria primitiva», eine real existierende, sehr erfolgreiche Lotterie in Spanien. Der Gewinn sei auszahlungsbereit, es müssten nur noch Formalitäten erledigt werden. Für die Erledigung dieser Formalitäten (Steuervorauszahlung, Anwaltshonorare, Bank-, Überweisungs- und Nachforschungsspesen etc.) wird vom Opfer eine substanzielle Vorleistung verlangt. Die Zahlungen müssen über einen Geldtransferdienst geleistet werden, z. B. «Western Union», «Moneygram» oder andere.

Der Lotteriegewinn wird selbstverständlich nie ausbezahlt, und auch die geleisteten Vorschüsse werden nicht zurückbezahlt. Das Opfer wird mit immer neuen Vorwänden um Zahlung gebeten. Dabei kommen auch gefälschte Briefe und Dokumente von angesehenen Firmen (häufig Bankinstitute) und wichtigen Behörden (Europol, Interpol) zum Einsatz. Die Schadenssumme geht rasch in die Tausenden von Franken, der SKP sind Fälle bekannt, in denen bis zu 250 000 Franken an Vorschüssen ins Ausland überwiesen wurden.

Ähnliche Formen: Vorschussbetrug mit Erbschaften aus dem Ausland, Vorschussbetrug mit dem Transfer des Vermögens von bekannten Potentaten über unverdächtige Konten in der Schweiz.

2. Wohnungsmiete-Vorschussbetrug

Vitaly Krivosheev/123RF

Die Betrüger schalten auf bekannten Immobilienportalen glaubhafte Annoncen für tolle Mietwohnungen in fantastischer Lage zu einem günstigen Preis. Dabei werden Objekte angeboten, die im Moment gar nicht zur Vermietung stehen. Die Annoncen wurden aus einem früheren Vermietungsversuch auf dem Immobilienportal kopiert und aufbewahrt, um später bei einem Vorschussbetrug benutzt werden zu können. Es ist auch möglich, dass das Mietobjekt gar nicht existiert.

Auf die Anfrage des interessierten Mieters (und zukünftigen Betrugsopfers) antwortet der Betrüger, er sei im Moment im Ausland und benötige die Wohnung nicht, er möchte sie deshalb an vertrauenswürdige Personen vermieten. Die Wohnung könne vom Opfer selbständig besucht werden, zur Sicherheit müsse jedoch vorgängig mind. eine Monatsmiete als Kaution bezahlt werden. Es kann vom Betrüger auch eine Kaution für den Schlüssel verlangt werden. Weder die im Voraus bezahlte Monatsmiete noch die Kaution für den Schlüssel werden jemals wieder zurückbezahlt, noch ist das Mieten der angebotenen Wohnung möglich.

Ähnliche Formen: Vorschussbetrug mit der Miete von Einfamilienhäusern oder Büroflächen.

3. Ferien-Vorschussbetrug

Martin Valigursky/123RF

Die Betrüger haben auf bekannten Internetportalen Ferienwohnungen und -häuser ausgeschrieben, die gar nicht existieren. Der Betrüger versucht das Opfer aus dem Internetportal zu locken, damit die Vermietung vom Internetportal nicht überwacht werden kann. Die Betrüger locken mit reduzierter Miete, die Opfer werden gebeten, die Miete nicht über das Internetportal zu bezahlen, sondern die Miete über eine Bankanweisung oder einen Geldtransferdienst direkt zu überweisen. Es kann vom Betrüger auch eine Kaution für den Schlüssel verlangt werden. Weder die im Voraus bezahlte Miete noch die Kaution für den Schlüssel werden jemals wieder zurückbezahlt. Natürlich steht das Opfer an der Feriendestination auch ohne Unterkunft da, in der Hochsaison eine durchaus dramatische Situation.

4. Fahrzeug-Vorschussbetrug

zvg

Die Betrüger platzieren ein Verkaufsinserat für ein Fahrzeug in den bekannten Internetportalen. Das Opfer, das sich beim Betrüger meldet, um das Fahrzeug des Betrügers zu kaufen, wird vom Betrüger informiert, dass er eine Transportfirma mit dem Versand des

Fahrzeugs beauftragen wird. Die Transportfirma, die ebenfalls zum Netzwerk des Betrügers zählt, meldet sich kurz darauf bei der Käuferin oder dem Käufer und verlangt Adresse und weitere Infos zur Käuferin oder zum Käufer. Anschliessend wird auch noch ein Vorschuss auf den Versand und unter Umständen sogar der Verkaufspreis eingefordert, bevor das Fahrzeug geliefert wird. Selbstverständlich wird weder das Fahrzeug geliefert, noch werden Transportkosten oder der Verkaufspreis zurückerstattet.

Ähnliche Formen: Vorschussbetrug mit anderen Artikeln, die auf den Internet-Portalen verkauft werden.

Wie häufig kommt Vorschussbetrug vor?

Es existieren keine statistischen Angaben zur Häufigkeit des Vorschussbetrugs. In einer Statistik eingeschlossen sind nur Fälle, die der Polizei durch Anzeige zur Kenntnis gebracht werden. In vielen Fällen von Vorschussbetrug verzichtet das Opfer auf eine Anzeige, weil es von vornherein unmöglich scheint, den Täter je zu finden, oft weil sich der Täter aus dem Ausland gemeldet hat. Opfer verzichten auch aus Scham auf eine Anzeige bei der Polizei, weil es im Nachhinein selbst für das Opfer nicht mehr verständlich ist, wieso man auf den Betrug hereinfallen konnte. Auch Betrugsversuche werden fast nie bei der Polizei gemeldet. Aus diesen Gründen ist nicht feststellbar, wie häufig Vorschussbetrug vorkommt. Aufgrund der häufigen Anfragen von Einwohnerinnen und Einwohnern zu Möglichkeiten der Ermittlung gegen Vorschussbetrug geht die SKP von einem riesigen Dunkelfeld aus. Zudem muss die Deliktsumme sehr hoch sein, wenn die genannten Betrugssummen hochgerechnet werden.

Besondere Problematik beim Vorschussbetrug

Die Tricks der Betrüger ändern sich sehr rasch, es ist fast unmöglich, den Überblick über alle möglichen Vorschussbetrugsformen zu behalten. Zudem nutzen Vorschussbetrüger oft die Namen von bekannten und seriösen Firmen und versuchen unter deren Namen die Betrogenen zu verwirren und an weitere persönliche Informationen zu gelangen.

Jeder Art von Vorschussbetrug liegt folgendes Problem zugrunde: Ist das Geld einmal ausbezahlt, ist es fast unmöglich, das Geld zurückzufordern. In den meisten Fällen verlieren die Geschädigten ihr Geld für immer.

Die Verfolgung der Vorschussbetrüger ist aufgrund folgender Punkte in der Regel sinnlos:

- Vorschussbetrüger agieren meist aus dem Ausland, mit falschem Namen und nicht registrierten Telefonnummern und E-Mail-Adressen. Die Täter sind nicht bekannt.
- Sind die Vorschussbetrüger im Ausland bekannt und könnten sie zur Verantwortung gezogen werden, kann unter Umständen ein schlecht funktionierendes Strafverfolgungssystem in diesem Land eine Verfolgung unmöglich machen (Korruption).
- Hätten sich die Betrogenen mit einem Mindestmass an Aufmerksamkeit vor dem Betrug schützen oder ihren Irrtum durch ein Minimum an zumutbarer Vorsicht vermeiden können, dann liegt im Sinne des Strafgesetzbuches kein Betrug vor. Dem Betrüger kann keine Arglist vorgeworfen werden (siehe dazu BGE 126 IV 165).

Dennoch ist es unerlässlich, dass die Polizei in jedem Fall abklärt, ob das Verhalten der Vorschussbetrüger tatsächlich strafbar ist. Je nach Fall liegt ein Betrug in Sinne von Artikel 146 vor.

Präventionsmassnahmen gegen Vorschussbetrug

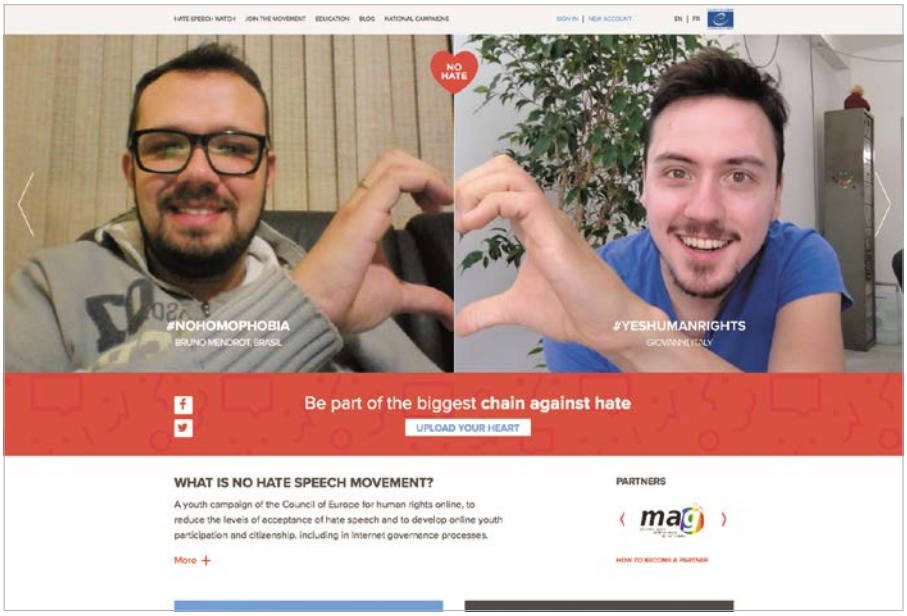
- Zahlen Sie keine Vorschüsse für Waren oder Dienstleistungen.
- Beharren Sie, vor allem bei höheren Geldsummen, auf Übergabe der Ware zur gleichen Zeit wie die Zahlung. Am besten Treffen Sie sich mit dem Verkäufer, um die Ware abzuholen und gleich zu bezahlen.
- Nutzen Sie einen Escrow-Service (z. B. bei eBay möglich).
- Werden Sie misstrauisch, wenn Ihnen ein Angebot extrem attraktiv erscheint (sehr günstig, sofort verfügbar, «Schnäppchen»).
- Werden Sie auch misstrauisch, wenn ein Verkäufer Sie dazu drängt, einen Kauf möglichst rasch abzuschliessen, weil das Objekt sonst gleich anderweitig verkauft wird. Stress kann dazu führen, dass man es mit der Vorsicht nicht mehr ganz so genau nehmen kann.

«Hate Speech» (Hassreden)

Was versteht man unter «Hate Speech»?

Der Begriff «Hate Speech» umfasst jegliche Äusserungen oder Bilder, die andere Menschen beleidigen, ausgrenzen oder zu Gewalt gegenüber einem bestimmten Menschen oder einer Gruppe von Menschen aufrufen. Die beleidigenden Aussagen oder Bilder basieren oft auf dem Geschlecht, der Religion, der Herkunft, bestimmten körperlichen Attributen oder der sexuellen Orientierung eines Menschen oder einer Gruppe oder Kombinationen dieser Faktoren. Der Vielfalt von «Hate Speech» sind keine Grenzen gesetzt. «Hate Speech» kann sich deshalb an einzelne Personen wie beispielsweise ein übergewichtiges Mädchen oder einen Rollstuhlfahrer, aber auch an grössere Gruppen wie Muslime oder Menschen dunkler Hautfarbe richten. Gleichzeitig werden stets neue Personen oder Gruppen durch «Hate Speech» angegriffen. Auf der anderen Seite kann jeder, der sich gesellschaftlich exponiert, sei es beruflich oder als Privatperson, und/oder eine polarisierende öffentliche Aussage macht, ein Opfer von «Hate Speech» werden.

Die Folgen von «Hate Speech» können unterschiedlich ausfallen. Für Einzelpersonen wie das übergewichtige Mädchen können diese Angriffe eine grosse emotionale Belastung bedeuten. Findet «Hate Speech» auf Kosten einer Gruppe von Menschen statt, so führt



Website «No Hate Speech», eine Kampagne des Europarates, https://www.nohatespeechmovement.org

dies vor allem zu einer Stigmatisierung der Gruppe und der Förderung von möglichen negativen Stereotypen.

Wie häufig kommt «Hate Speech» vor?
Der Ort, an dem «Hate Speech» am schnellsten verbreitet wird, ist das Internet. Soziale Netzwerke, Blogs oder Kommentarspalten ermöglichen ihren Nutzern, sich zu den unterschiedlichsten Themen frei zu äussern und darüber zu diskutieren. Diese virtuelle Meinungsfreiheit wird jedoch oft auch ausgenützt, indem extreme und diskriminierende Aussagen von Einzelpersonen oder Gruppierungen in den Sozialen Medien platziert werden. Zudem führen der fehlende physische Kontakt sowie die partielle Anonymität im Netz dazu, dass die Hemmschwelle in vielen Online-Communities (ohne Diskussionsregeln) sinkt. Auf diese Weise trauen sich Menschen plötzlich, Dinge zu schreiben, die sie ihren Mitmenschen niemals persönlich sagen würden.

Die Anonymität der Täter und Täterinnen in Kombination mit den Verbreitungsmechanismen des Internets erschweren das Aufspüren der Quellen von «Hate Speech» und somit auch die Dokumentation der Delikte und Aussagen über die Häufigkeit der Anzeigen. Verschiedene Untersuchungen konnten jedoch aufzeigen, dass «Hate Speech» ein verbreitetes Phänomen ist und wer davon betroffen ist. Im Jahr 2015 zum Beispiel hat der Europarat eine Online-Meinungsumfrage zum Thema «Hate Speech» durchgeführt. Die Umfrage ergab, dass 83 % der Befragten online bereits Erfahrungen mit «Hate Speech» gemacht hatten. Die Hauptzielgruppen von Hasskommentaren waren gemäss der Umfrage: LGBTI-Jugendliche[3], Muslime und Musliminnen sowie Frauen allgemein.

Präventionsmassnahmen gegen «Hate Speech»
«Hate Speech» hat vor allem mit der Verbreitung von Hass zu tun. Mit dem Aufkommen der Sozialen Medien ist dies sehr einfach geworden. Jede Person, die schreiben kann, kann im Internet ihre Meinung kundtun und (un)-willentlich zum «Hater» werden. Aus diesem Grund sollte man immer darüber nachdenken, ob die eigenen Kommentare oder Aussagen niemanden beleidigen oder ausgrenzen oder allenfalls andere Personen zu negativen Aussagen provozieren. Ausserdem sollten keine Meinungen oder Inhalte geteilt werden, die unreflektiert und extrem sind oder allenfalls verboten, wie Aufrufe zur Gewalt (Bundesgesetz über Massnahmen zur Wahrung der inneren Sicherheit) oder die Unterstützung von verbotenen Organisationen wie der Al-Qaida oder des Islamischen Staats (Bundesgesetz über das Verbot der Gruppierungen «Al-Qaïda» und «Islamischer Staat» sowie verwandter Organisationen).

Es gibt jedoch auch verschiedene Möglichkeiten, um im Nachhinein gegen «Hate Speech» vorzugehen. Es liegt nicht nur an den Opfern, sich zu wehren, sondern auch an den Zeugen und Zeuginnen, sich zivilcouragiert zu verhalten und sich gegen Diffamierung und/oder Diskriminierung stark zu machen.

- Wenden Sie sich während oder nach einem Vorfall an Ihre Familie, Bekannte oder eine Beratungsstelle und besprechen Sie beleidigende Äusserungen, die an Sie gerichtet sind oder die über andere verbreitet werden.
- Blockieren Sie Nutzerinnen und Nutzer, die diffamierende und/oder diskriminierende Aussagen im Internet verbreiten, damit diesen Personen keine Verbreitungsmöglichkeiten mehr gegeben werden.
- Erstatten Sie bei den jeweiligen Plattformprovidern, wie Facebook oder Instagram, eine Meldung über die Verbreitung von diskriminierenden und/oder diffamierenden Äusserungen.
- Wenn Sie strafrechtlich gegen die Person oder eine Gruppe vorgehen möchten, erstatten Sie Anzeige bei der Kantonspolizei. Es empfiehlt sich jedoch, vorab bei einer Beratungsstelle abzuklären, ob dieser Schritt auch wirklich sinnvoll ist.
- Bewahren Sie die Beweismittel, wie zum Beispiel Screenshots mit Zeit-

3 LGBTI ist eine aus dem englischen Sprachraum kommende Abkürzung für Lesbian, Gay, Bisexual, Transgender and Intersex, also Schwule, Lesben, Bisexuelle, Transgender und Intersexuelle.

stempel und URL, Chatprotokolle oder Bilder, die den Vorfall dokumentieren, unbedingt auf.

Mehr Informationen zum Thema:

Jugend und Medien – Das Informationsportal zur Förderung von Medienkompetenz in der Schweiz: www.jugendundmedien.ch → Chancen und Gefahren → Gefahren im Überblick → Extremismus

«No Hate Speech»-Kampagne des Europarates in Deutschland: no-hate-speech.de

Identitätsdiebstahl und -missbrauch

Heute will kaum jemand in der Schweiz auf die Benutzung des Internets verzichten: Die allermeisten von uns verfügen über mindestens einen privaten E-Mail-Account und nutzen ihn, um Nachrichten an Verwandte und Freunde zu verschicken und Nachrichten von ihnen zu empfangen. Immer mehr Bürgerinnen und Bürger verzichten auf den monatlichen Gang zur Bank und Post und erledigen ihre Rechnungen mittels E-Banking. Auch das Einkaufen in Online-Shops im In- und Ausland sowie die Möglichkeit, sich vom Schreibtisch aus beruflich zu vernetzen, schätzen viele. Mit anderen Worten: Die Digitalisierung unseres Alltags findet statt und hat zur Folge, dass es zahlreiche Daten von uns im Internet gibt.

Es geht meistens ums Geld und manchmal um Rufschädigung

Wenn unsere Daten in fremde Hände gelangen und missbraucht werden, spricht man von Identitätsdiebstahl oder Identitätsmissbrauch. Wenig überraschend werden Daten grossmehrheitlich gestohlen und missbraucht, um sich mit Hilfe dieser zu bereichern. Denken wir dabei zum Beispiel an Kreditkartendaten, mit denen man heute leicht online Hotelzimmer bezahlen und Kleider, Wein oder sonstige Produkte online kaufen und an eine beliebige Adresse liefern lassen kann. Es kommt auch vor, dass Daten gestohlen und missbraucht werden, um den Ruf der bestohlenen Person zu schädigen: Der Täter oder die Täterin gibt sich in den Weiten des Internets als das Opfer der bestohlenen Person aus, erstellt beispielsweise Fake-Accounts in den Sozialen Netzwerken oder bietet im Namen des Opfers der bestohlenen Person auf einschlägigen Webseiten sexuelle Dienstleistungen an.

everythingpossible/123RF

Mit gestohlenen Kreditkartendaten kann man heute leicht online Hotelzimmer bezahlen und Kleider, Wein oder sonstige Produkte kaufen.

Daten einsammeln oder erbeuten

Zweifellos wird der Identitätsdiebstahl oder -missbrauch den Täterinnen und Tätern in manchen Fällen sehr leicht gemacht. Gewisse Daten müssen im Internet weder erbeutet noch gestohlen, sondern lediglich «eingesammelt» werden. Einige Userinnen und User sind so offen und sorglos, dass sie in ihren Social-Media-Accounts private Fotos, ihre Telefonnummer und Adresse, ihr Geburtsdatum, die Namen ihrer Familienmitglieder und ihres Arbeitsgebers für jedermann zugänglich machen. Andere gestatten solche Einblicke zwar nur ihren Freunden, aber nehmen gleichzeitig Freundschaftsanfragen an, ohne die entsprechende Person im «Real Life» jemals getroffen zu haben. An Kredit- und Bankdaten zu gelangen ist zwar weitaus schwieriger, aber dennoch gelingt es Kriminellen häufig, zum Beispiel mit Hilfe von Phishing-Mails, ahnungslose Bürgerinnen und Bürger dazu zu bewegen, sensible Daten preiszugeben.

Individuelle Vorsicht schützt nur bedingt

Wer jetzt denkt, man könne sich vor Identitätsdiebstahl und -missbrauch schützen, indem man auf die Nutzung des Internets verzichtet, macht sich leider etwas vor. Inzwischen sind nämlich zahlreiche sensible Daten über jeden Einzelnen von uns im Internet. Natürlich sind unsere Bankdaten, unsere Krankenakten und dergleichen gut geschützt, aber menschliches Versagen (zum Beispiel das Ablegen eines Datenpakets auf dem falschen Server) oder ein Hack können dazu führen, dass unsere Daten missbraucht werden, ohne dass wir dies durch individuelle Vorkehrungen hätten verhindern können.

Präventionsmassnahmen

Obwohl das Internet für uns also ein gewisses Risiko mit sich bringt, Opfer eines Identitätsdiebstahls zu werden, kann jede Bürgerin und jeder Bürger dieses Risiko durch bestimmte Verhaltensweisen und technische Vorkehrungen minimieren:

- Auf der Webseite der Melde- und Analysestelle Informationssicherung MELANI findet man zahlreiche Tipps und Hinweise, wie man die eigenen Daten und Geräte vor Diebstahl und Angriffen schützen kann.
  www.melani.admin.ch
- Auf der Webseite der Koordinationsstelle zur Bekämpfung der Internetkriminalität KOBIK kann man sich über die häufigsten Modi Operandi im Internet informieren und nachlesen, vor welchen betrügerischen E-Mails und Webseiten aktuell gewarnt wird.
  www.cybercrime.admin.ch

Der Identitätsdiebstahl oder -missbrauch findet im Schweizer Strafgesetzbuch StGB keine explizite Erwähnung. Solche Diebstähle und Missbräuche gehen jedoch immer mit strafrechtlich relevanten Handlungen einher. Dazu gehören (je nach Art des Diebstahls oder Missbrauchs) u. a. die unbefugte Datenbeschaffung (Art. 143 StGB), das unbefugte Eindringen in ein Datenverarbeitungssystem (Art. 143bis 126 StGB) und strafbare Handlungen gegen die Ehre und den Geheim- oder Privatbereich (Art. 173ff. StGB).

Die Stadtpolizei Zürich und ihre Social-Media-Strategie: Von ICoP bis Instagram

Ein Interview mit Michael Wirz, Chef des Fachbereichs Kommunikation der Stadtpolizei Zürich

Herr Wirz, seit vielen Jahren nutzt die Stadtpolizei Zürich die digitalen Medien, um die Bevölkerung der Stadt mit aktuellen Informationen zu versehen. Wieso hat sich die Stadtpolizei entschieden, in den Sozialen Medien aktiv zu werden?

Im Jahr 2008 verabredeten sich zahlreiche Personen via Facebook zu einem Botellón in Zürich. Über tausend Jugendliche und junge Erwachsene nahmen schliesslich an diesem «Massenbesäufnis» teil und verursachten für die ganze Stadtverwaltung Kosten von mehreren hunderttausend Franken. Damals wurde uns zum ersten Mal klar, dass wir uns mit Facebook auseinandersetzen müssen. Im Auftrag des Kommandanten habe ich von 2009 bis 2011 eine Strategie ausgearbeitet und dazu eine Umfrage in der Online-Community durchgeführt. Ich war über den grossen Zuspruch erstaunt: Die Befragten waren sehr daran interessiert, mit der Polizei via Soziale Medien zu kommunizieren. Heute sind wir auf Facebook, Twitter, YouTube und Instagram aktiv.

Welche Strategie und welche Ziele werden mit der Nutzung der Social-Media-Kanäle verfolgt?

Zuerst einmal wollen wir mit der Bevölkerung in einen Dialog treten und die Social-Media-Kanäle deshalb nicht einfach als zusätzliche Distributionsmöglichkeit für Medienmitteilungen usw. einsetzen. Sehr viele Bürgerinnen und Bürger nutzen heutzutage Soziale Medien, darum müssen wir als Polizei auch dort präsent sein. Das bedeutet, dass wir die Philosophie und Kultur, die wir ausserhalb des Internets leben, auch konsequent online umsetzen. Im Grunde genommen ist die polizeiliche Arbeit im Internet und im Alltag dieselbe. Wir führen unsere Kommunikationsstrategie weiter und haben sie lediglich ergänzt. So bleiben wir authentisch, zielgerichtet und schaffen Vertrauen. Zu Beginn haben wir die Inhalte vorgängig geplant (content plan). Das hat uns jedoch zu sehr eingeschränkt. Heute «posten» wir dann, wenn etwas passiert, und wir haben festgestellt, dass es für unsere Facebook-Freunde und Abonnenten kein Problem ist, wenn zwei Wochen nichts Neues kommt.

Welcher Kanal eignet sich für welche Nutzung?

Twitter nutzen wir zur zeitnahen und direkten Information. Wir erreichen damit besonders gut Meinungsbildner wie Medienschaffende, Politikerinnen und Politiker, aber auch verschiedene Organisationen. Twitter ermöglicht uns, in manchen Fällen auch ein Stück weit Einfluss auf das Agenda-Setting zu nehmen. Weil es etwas «lockerer» zu- und hergeht, kann man manchmal ein Thema anstossen, das man sonst weniger ansprechen kann.

Facebook funktioniert sehr gut für etwas längere, tiefergehende Geschichten, oftmals mit Bildern. Wir holen dort auch die Meinung und die Befindlichkeit der Bevölkerung ab und geben einen Einblick hinter die Kulissen der Polizeiarbeit. Thematisch nutzen wir unsere Kanäle und deren grosse Reichweite aber auch, um Präventionsbotschaften zu verbreiten.

Kann man über Soziale Medien das Vertrauen der Bevölkerung gewinnen?

Natürlich nicht alleine, das Verhalten im direkten Kontakt ist genauso wichtig. Wenn ich die Reaktionen und die zahlreichen Anfragen betrachte, die wir auf diesen Kanälen erhalten, bin ich aber davon überzeugt, dass das Engagement zur Vertrauensbildung beiträgt! Wir behandeln das uns entgegengebrachte Vertrauen sehr sorgfältig und gehen den Anfragen sehr seriös und detailliert nach. Wir achten zudem darauf, dass die Inhalte, die wir verbreiten, zu 100 % verlässlich sind.


zvg

Michael Wirz ist Chef des Fachbereichs Kommunikation der Stadtpolizei Zürich. Der 40-jährige ausgebildete Polizist hat sich in den letzten Jahren intensiv mit dem Thema «Digitalisierung und Polizeiarbeit» auseinandergesetzt. Er hat insbesondere die Chancen und Risiken des Social-Media-Einsatzes für Blaulichtorganisationen im Rahmen seiner Masterarbeit untersucht und bei der Stadtpolizei Zürich den Einsatz der neuen Medien strategisch geplant und eingeführt. Das Korps hat inzwischen in diesem Bereich eine führende Rolle in den deutschsprachigen Ländern Europas eingenommen. Michael Wirz ist zudem Dozent für Verwaltungskommunikation an verschiedenen Fachhochschulen.

Patrick Jean ist der erste ICoP der Schweiz. Wie entstand diese Idee eines Internet-Community-Polizisten?
Wenn man ein Anliegen hat, will man grundsätzlich lieber mit Menschen und nicht mit anonymen Organisationen reden. Das ist online nicht anders als offline. Auf einer Tagung des European Police College (cepol) haben wir den finnischen «nettipoliisi» Marko Forrs kennengelernt. Dabei handelt es sich um einen Kollegen aus Helsinki, der seit vielen Jahren online unterwegs ist.

Der ICoP Patrick Jean auf Facebook.

Diese Idee des Online-Community-Policing faszinierte mich und ich wollte herausfinden, ob das auch in der Stadt Zürich funktioniert. Wir machten uns also auf die Suche nach einem geeigneten Kollegen. Patrick Jean war zu dieser Zeit in unserer Abteilung im Praktikum und schien dafür gut geeignet. Er ist kommunikativ, offen, hat einen guten Schreibstil und das notwendige Fingerspitzengefühl. Wir haben ihn entsprechend ausgebildet und schliesslich einen sechsmonatigen Pilotversuch gestartet. Das Interesse und das Vertrauen in ihn als ICoP war riesig und er hatte rasch viele «Freunde» und Follower! Heute wird er sogar häufig von Teenies und jungen Leuten auf der Strasse erkannt und angesprochen. Er arbeitet 50 % als Quartierpolizist in Zürich-Hottingen und 50 % als ICoP.

Welche Weiterentwicklungen sind geplant beziehungsweise schon in Gange?
Seit Juli dieses Jahres gibt es mit Eleni Moschos auch ein weibliches Pendant zu Patrick Jean. Zum einen entlastet ihn das und zum anderen gibt es Themen und Bereiche, bei denen Eleni als Frau besseren Zugang hat. Man darf nicht vergessen, dass Patrick und Eleni vor allem im Hintergrund arbeiten, indem sie Direktnachrichten, die sie über Facebook erreichen, bearbeiten und so unbürokratisch beratend und schlichtend tätig sind. Sie fungieren häufig als Türöffner für Jugendliche und junge Menschen, die sich bei ihnen via Facebook oder Instagram melden. Es kommt immer wieder vor, dass sie beispielsweise Termine beim Jugenddienst vereinbaren oder sie an eine geeignete Beratungsstelle weiterweisen. Frauen und Mädchen wollen sich, wenn sie die Wahl haben, bei gewissen Themen lieber einer Frau anvertrauen.

Was die Nutzung von neuen Plattformen und Kanälen anbelangt, bleiben wir immer am Ball. Wir prüfen derzeit Plattformen wie Snapchat und Periscope und beschäftigen uns viel mit Online-Videos.

Welche Probleme mussten Sie schon meistern? Gab es schon Shitstorms, Drohungen gegen die Stadtpolizei, Persönlichkeitsverletzungen und ähnliches?
Einen Shitstorm hatten wir noch nie. Es ist aber schon einmal vorgekommen, dass wir 50 negative Kommentare in Zusammenhang mit einem «Post» über ein Sicherheitskonzept für einen Fussballmatch hatten. Wir hatten das aber bis anhin gut im Griff und haben uns die Zeit genommen, einzeln auf die Kommentare zu antworten.

Hin und wieder gibt es aber auch Persönlichkeitsverletzungen: User laden beispielsweise das Foto eines falsch parkierten Autos vor ihrem Haus hoch. Wir klären sie dann auf und bitten sie, das Foto zu löschen.

Was für ein Fazit ziehen Sie, nachdem Ihr Korps bereits mehrere Jahre lang auf und mit Sozialen Medien arbeitet: Tragen die Sozialen Medien dazu bei, die Arbeit der Polizei zu erleichtern oder ist das Engagement in den Sozialen Medien in erster Linie eine zusätzliche Aufgabe?
Ich ziehe insgesamt eine positive Bilanz und bin überzeugt, dass es unsere Arbeit erleichtert. Was wir in den Sozialen Medien machen, ist nämlich weit mehr als nur PR, es ist Community Policing. Es ist also eigentlich normale Polizeiarbeit, einfach online. Wir gehen online genauso pragmatisch vor wie offline. Ich erinnere mich beispielsweise an einen Fall, bei dem wir einen Vermissten eher zufällig auf Facebook fanden und ihm kurzerhand eine Nachricht schickten. Er meldet sich zurück, es sei alles in Ordnung, er sei im Ausland und melde sich sofort bei seinen Angehörigen. In diesen Fällen kann es die Polizeiarbeit erleichtern und so insgesamt sogar entlastend sein. Die ganze Social-Media-Arbeit ist natürlich auch ein Transparenzversprechen und so eine vertrauensbildende Massnahme, was wir an den zahlreichen Anfragen erkennen. Es kommt zum Beispiel immer wieder vor, dass uns Leute auf den Sozialen Medien zu verstehen geben, dass sie von der Polizei eigentlich nicht viel halten, aber gut finden, was wir machen.

Ich würde es interessant finden, wenn in Zukunft auch andere Korps Online-Polizisten einsetzen würden, denn unsere ICoPs haben auch Freunde ausserhalb der Stadt und des Kantons Zürich und da wäre es manchmal hilfreich, wenn man diese Bürger weiter weisen könnte. Interesse an unserer Tätigkeit aus anderen Korps spüren wir schon heute. Ganz nach dem Grundprinzip der Sozialen Medien geben wir unsere Erfahrungen gerne an andere weiter, denn Wissen ist das einzige Gut, das sich durch Teilen nicht vermindert, sondern vermehrt!

Facebook www.fb.com/StadtpolizeiZH
Twitter @StadtpolizeiZH

ICoPs der Stadtpolizei Zürich
Patrick Jean
Facebook www.fb.com/stapojean
Instagram @stapojean

Eleni Moschos
Facebook www.fb.com/eli.stapo
Instagram @eli.stapo

Informationsmaterialien der SKP

Prävention mit Fokus auf digitale Medien ist aus verschiedenen Grünen wichtig und nützlich. Kinder und Jugendliche wachsen heutzutage off- und online auf und müssen sich dementsprechend Kompetenzen in der realen und auch in der digitalen Welt aneignen. Viele Betrugsarten im Netz sind relativ einfach durchschaubar, wenn man sie denn kennt. Information ist deshalb oft bereits eine hinreichende Präventionsmassnahme. Und wenn Bürgerinnen und Bürger ganz grundsätzlich lernen und verstehen, wie das Internet funktioniert und wie getrickst und «gefaket» werden kann, steigt die Wahrscheinlichkeit deutlich, kriminelle Machenschaften zu durchschauen.

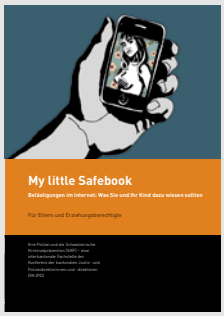
Die Schweizerische Kriminalprävention hat deshalb einige Broschüren und Flyer erarbeitet, die diesen Umständen und Zielgruppen Rechnung tragen.

Die verschiedenen Produkte können auf der Webseite www.skppsc.ch heruntergeladen oder bei den Kantons- und Stadtpolizeien bezogen werden.

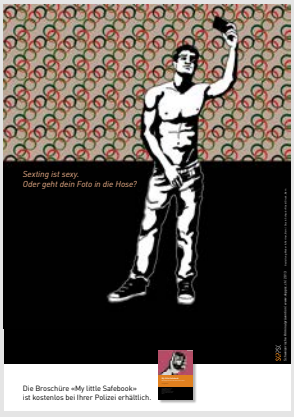
Broschüre «My little Safebook»
für Jugendliche

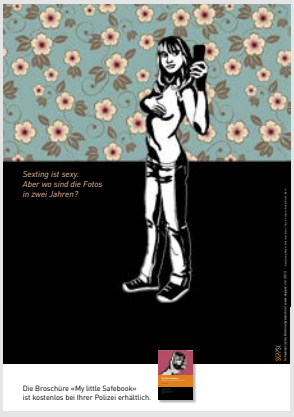
«My little Safebook» richtet sich an Jugendliche ab 12 Jahren und erklärt ihnen, was sie über Belästigungen im Internet wissen müssen. Die Broschüre zeigt auf, wie sich Jugendliche vor Cybermobbing, sexuellen Übergriffen und Abo-Fallen im Internet schützen können und leitet sie zudem an, den eigenen Medienkonsum kritisch zu reflektieren und über den Unterschied zwischen der realen und der virtuellen Welt nachzudenken. Ergänzt wird die Broschüre durch eine kurze Übersicht der rechtlichen Rahmenbedingungen sowie Links zu weiterführenden Informationen.

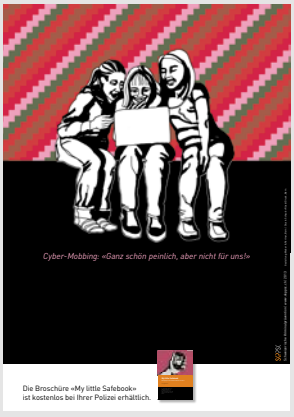
Broschüre «My little Safebook»
für Eltern



«My little Safebook» richtet sich an Eltern und Erziehungsberechtigte von Jugendlichen ab 12 Jahren. Es hilft ihnen zu verstehen, warum das Internet Jugendliche fasziniert und wie man sie in den Sozialen Netzwerken kompetent begleitet. Die Broschüre informiert detailliert über Cybermobbing, sexuelle Übergriffe und Abo-Fallen im Internet und zeigt auf, wie Jugendliche sich davor schützen können. Sie spricht die Themen Medienkonsum und Medienkompetenz an und erklärt, wie sich ein vorbildlicher Erwachsener im Internet verhalten sollte. Ergänzt wird die Broschüre durch eine kurze Übersicht der rechtlichen Rahmenbedingungen sowie Links zu weiterführenden Informationen.







Poster A3 «Sexting» und «Cybermobbing»

«Sexting ist sexy. Oder geht dein Foto in die Hose?»

«Sexting ist sexy. Aber wo sind die Fotos in zwei Jahren?»

«Cyber-Mobbing: Ganz schön peinlich, aber nicht für uns!»

Broschüre «Es war einmal ... das Internet»

Kinder kommen immer früher in Kontakt mit dem Internet. Die Broschüre «Es war einmal ... das Internet» richtet sich deshalb an Eltern von Kindern unter 12 Jahren.
Fünf moderne Märchen sprechen auf witzige Weise die fünf wichtigsten Problembereiche an: Internetsucht, Pädokriminalität, Cybermobbing, Online-Shopping und Abonnementsfallen sowie Datenschutz. Die illustrierten Märchen kann man vorlesen oder sie können von Kindern selbst gelesen werden. Die kurzen Kapitel «Und die Moral von der Geschicht'» zeigen den Eltern bei jedem Problembereich die Hintergründe und geben Verhaltenstipps.

«Cybermobbing: Alles, was Recht ist»

Das Faltblatt «Cybermobbing: Alles, was Recht ist» gibt Auskunft über die wichtigsten Gesetzesartikel zum Thema Cybermobbing. Zwei Fallbeispiele erläutern, wie über die neuen Medien gemobbt wird und sieben Empfehlungen zeigen auf, wie gegen Cybermobbing vorgegangen werden kann. Das Faltblatt hat ausserdem zum Ziel, dass Jugendliche die Grenze zwischen Streitereien und Cybermobbing erkennen. Eltern und Erziehungsberechtigten soll dieses Faltblatt Sicherheit in der Diskussion über dieses Thema zu geben.

«Pornografie: Alles, was Recht ist»

Das Faltblatt «Pornografie: Alles, was Recht ist» informiert über die wichtigsten Gesetzesartikel zum Thema Pornografie im Internet. Das Faltblatt erläutert die Gesetzeslage und liefert Eltern und Jugendlichen wichtige Informationen zu den Themen Schutzalter, Sexting und illegale Pornografie. Es soll ausserdem Eltern und Erziehungsberechtigten Sicherheit in der Diskussion über dieses Thema geben.

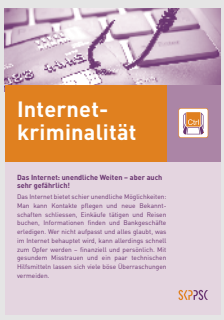
«Das eigene Bild: Alles, was Recht ist»

Das Faltblatt «Das eigene Bild: Alles, was Recht ist» zeigt mit Fallbeispielen auf, unter welchen Bedingungen das Recht am eigenen Bild verletzt wird und wie dagegen vorgegangen werden kann. Es erklärt die gesetzlichen Grundlagen und beschreibt, in welchen Fällen Gerichte von einer stillschweigenden Einwilligung ausgehen. Das Faltblatt informiert darüber, was beim Fotografieren von Kindern und Jugendlichen besonders beachtet werden muss, um die Rechte am eigenen Bild von Minderjährigen nicht zu verletzen.

«Checkliste – Sicherheit in Sozialen Netzwerken»

Auf einer Doppelseite gibt diese Checkliste fünf Hinweise zur Funktionsweise von Sozialen Netzwerken und vier Verhaltensempfehlungen, damit unliebsame Überraschungen ausbleiben und die Vorteile dieser Netzwerke gut genutzt werden können.

Postkarten «Internetkriminalität» und «Betrug»



Wechsel in der SKP-Leitungskommission

Die Leitungskommission genehmigt die Jahresplanung und die Jahresrechnung der SKP sowie die von der SKP-Geschäftsstelle zu erarbeitenden und umzusetzenden Präventionskampagnen.

Regierungsrätin Maya Büchi-Kaiser wechselte im Kanton Obwalden das Departement und trat deshalb per 30. Juni 2016 aus der Leitungskommission zurück. Ihre Nachfolge trat Regierungsrat **Christoph Amstad,** Vorsteher des Justiz- und Sicherheitsdepartements des Kantons Obwalden, an. Herr Amstad nimmt zudem die Vertretung des Polizeikonkordats Zentralschweiz in der Leitungskommission wahr.

Adrian Lobsiger, Vizedirektor fedpol, wurde zum neuen Eidgenössischen Datenschutz- und Öffentlichkeitsbeauftragen gewählt. Er verliess deshalb schon im Frühjahr 2016 die Leitungskommission. Die Vertretung der fedpol in der Leitungskommission wird neu von Vizedirektor **René Bühler** wahrgenommen.

Wechsel in der SKP-Projektkommission

Die Projektkommission beurteilt die Kriminalitätslage in der Schweiz und macht der Leitungskommission Vorschläge für die Kampagnenthemen. Sie nimmt zuhanden der Leitungskommission Stellung zu den Kampagnenkonzepten, bevor sie an die KKJPD weitergeleitet werden.

Robert Steiner war dasjenige Mitglied der Projektkommission mit den meisten Dienstjahren. Er nahm als Delegierter der Projektkommission an den Sitzungen der SKP-Leitungskommission teil. Dadurch war er das wichtige Verbindungsglied zwischen Leitungs- und Projektkommission

Er wurde als Chef der Kriminalpolizei des Kantons Wallis im Jahr 2016 pensioniert und daher an der Frühjahrssitzung 2016 aus der Projektkommission verabschiedet. An der Herbstsitzung 2016 der Projektkommission nahm bereits sein Nachfolger **Florian Walser,** Chef der Kriminalpolizei des Kantons Freiburg, teil. Florian Walser nimmt zudem die Vertretung der Chefs der Kriminalpolizeien des Polizeikonkordats Westschweiz wahr.

fedpol/Gaëtan Bally

Christoph Amstad

zvg

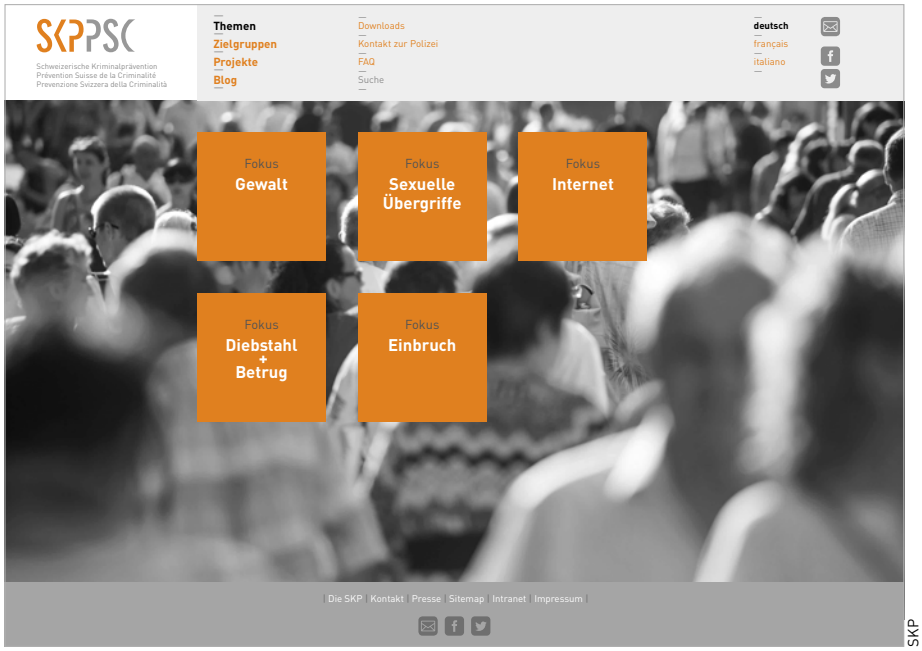
René Bühler

zvg

Florian Walser

Neuerarbeitung der SKP-Website

Am 1. Januar 2017 wird die neue Website der SKP aufgeschaltet. Die bisherige Themenstruktur war veraltet und musste komplett überarbeitet werden. Das heisst somit, dass bei allen Kooperationspartner der SKP, die auf ihren Websites eingefügten Direktlinks zu Inhalten der SKP-Website nicht mehr funktionieren werden und durch die Links auf die neuen Themenseiten ersetzt werden müssen. Die SKP versucht, ihre Kooperationspartner bereits vor der Umstellung über wichtige neue Links zu informieren.



SKP

Nationaler Aktionsplan (NAP) zur Verhinderung und Bekämpfung von Radikalisierung und gewalttätigem Extremismus

Der «Sicherheitsverbund Schweiz» (SVS) hat im Auftrag von Bund, Kantonen, Städten und Gemeinden mit der Ausarbeitung eines NAP begonnen. Er strebt das Ziel an, jegliche Art von Radikalisierung und gewalttätigem Extremismus zu verhindern. Der NAP umfasst vier unterschiedliche Handlungsfelder: Prävention, Repression, Schutz und Krisenvorsorge. Thematische Schwerpunkte, im Rahmen des NAP als Themenfelder bezeichnet, werden diesen Handlungsfeldern zugeteilt. Es werden neun unterschiedliche Themenfelder bearbeitet: Die Bearbeitung obliegt jeweils einer in diesem Themenfeld führenden Organisation. Folgende Themenfelder werden bearbeitet: Bildung, Integration, Anerkennung/Ausbildung, Sozialwesen, Sicherheit, interdisziplinäre Zusammenarbeit, Sensibilisierung, Deradikalisierung/Rehabilitation sowie internationale Zusammenarbeit.

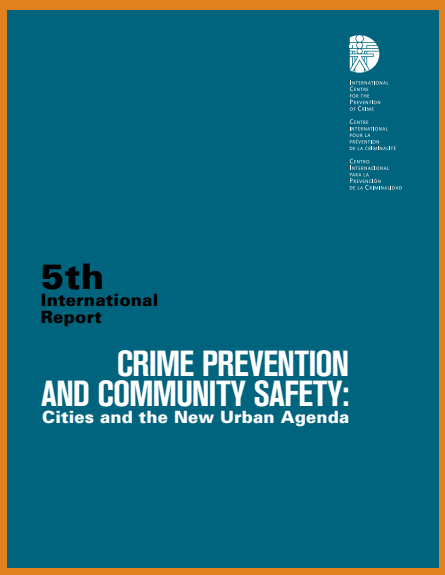
Die Erarbeitung des NAP soll bis spätestens Anfang September 2017 abgeschlossen sein. Im Juni 2017 wird eine Konsultation des NAP bei den zuständigen Behörden und Instanzen durchgeführt.

Mehr Informationen unter:
www.svs.admin.ch

5. Internationaler Bericht zu Kriminalprävention und öffentlicher Sicherheit

Das Internationale Zentrum für Kriminalprävention (ICPC) hat Anfang November 2016 seinen 5. Internationalen Bericht veröffentlicht. Er wurde mit «Städte und die neue urbane Agenda» betitelt und umfasst folgende Themen: «Neue Entwicklungen in der Kriminalität und ihre Prävention», «Urbane Sicherheit», «Städte, Bezirke und ihre Strategien für öffentliche Sicherheit anhand eines Beispiels aus Lateinamerika», «Kriminalprävention in städtischen Verkehrsmitteln», «Beziehung zwischen Kriminalprävention und Drogengebrauch im städtischen Umfeld» und «Städte und die Verhinderung von gewalttätiger Radikalisierung».

Der Bericht richtet sich vor allem an drei verschiedene Zielgruppen: an Entscheidungsträgerinnen und -träger und Parlaments- bzw. Regierungsmitglieder aus dem Sicherheitsbereich, an Expertinnen und Experten im Bereich Urbane Sicherheit sowie an die Forschungsgemeinschaft, die nach Good Practices sucht und Evaluationen durchführt und kommentiert. Der Bericht in englischer Sprache kann auf der Website des ICPC kostenlos heruntergeladen werden.



Mehr Informationen unter:
www.crime-prevention-intl.org

22. Deutscher Präventionstag 2017, Hannover, Deutschland

Der 22. Deutsche Präventionstag (DPT) findet am 19./20. Juni 2017 in Hannover statt. Das diesjährige Schwerpunktthema lautet «Prävention & Integration». Gastgebende Veranstaltungspartner sind das Bundesland Niedersachsen, die Landeshauptstadt Hannover und der Landespräventionsrat Niedersachsen (LPR). Die Anmeldung zum DPT erfolgt unter folgender Adresse:
www.praeventionstag.de → DPT 2017 in Hannover → Anmeldung.

Neuer Kurs beim Schweizerischen Polizei-Institut (SPI)
Urbane Sicherheit (6.40.00.d)

Zielgruppe

- Mitarbeitende von Gemeinde- und Stadtpolizeikorps, die Bewilligungen erstellen, prüfen und bearbeiten oder künftig damit beauftragt werden.
- Angehörige der kantonalen Polizeikorps (z. B. Postenchefs), die Gemeindebehörden in diversen Fachfragen zu Bewilligungen und Veranstaltungen beraten.
- Verwaltungsmitarbeitende, die sich mit Sicherheitsfragen bei Veranstaltungen und Bewilligungen auseinandersetzen.

Ziele

Die Teilnehmenden:

- erstellen den Ablauf eines Bewilligungsverfahrens für Veranstaltungen auf öffentlichem, halböffentlichem und privatem Grund und werden dazu befähigt, Bewilligungs- und Gesuchsformulare zu erklären und auszustellen;
- sind unter Zuhilfenahme von Checklisten und anderen Hilfsmitteln in der Lage, verschiedene Bewilligungsgesuche korrekt und effizient zu bearbeiten, Vernetzungsaufgaben wahrzunehmen und Schnittstellen zu definieren;
- werden durch einen Leitfall, den sie in der Gruppe bearbeiten, für spezifische Herausforderungen und Probleme bei Veranstaltungen sensibilisiert und können eigenständig entsprechende Problemlösungen erarbeiten;
- eignen sich mehr Wissen in den Bereichen Gesuche und Bewilligungen, Verwaltungsrecht, Crox Management, technische Überwachung im öffentlichen Raum und urbane Sicherheit an und können dies umsetzen.

Inhalte

Urbane Sicherheit; Bewilligungsverfahren für Veranstaltungen; Bewilligungs- und Gesuchsformulare; Verwaltungsrecht, Haftungsfragen als Bewilligungsinstanz, Festwirtschafts-,

Gastwirtschaftsbewilligungen, Alkohol & Jugendschutz; Crowd Management; Feuerpolizeiliche Vorschriften, OK Verantwortliche und ihre Pflichten; Technische Überwachung des öffentlichen Raumes; Eventkonzepte.

Der Kurs wird nur in deutscher Sprache durchgeführt.

www.edupolice.ch → kurse → kursangebot → 6.40.00.d Urbane Sicherheit

Neuer Direktor des SPI gewählt: Reto Habermacher

Anfang Oktober 2016 hat **Reto Habermacher** die Funktion des SPI-Direktors von Pius Valier übernommen. Das Schweizerische Polizei-Institut leitet im Auftrag der KKJPD das Projekt BGK 2020 und führt parallel dazu die entsprechenden Anpassungen seiner eigenen Organisation durch. Dieses Reorganisationsprojekt, das BGK 2020 und die Führung des SPI selber ergeben ein Pensum, das weit über 100 % liegen würde. Reto Habermacher wird neben der Führung des SPI das interne Reorganisationsprojekt leiten. Pius Valier hat sich auf Anfrage bereit erklärt, als operativer Projektleiter BGK 2020 im Rahmen eines externen Mandates im Auftrag der Strategischen Projektleitung in einem Teilzeitpensum tätig zu sein.

zvg

Mehr Informationen unter:
www.institut-police.ch

Jugend und Medien – das Informationsportal zur Förderung von Medienkompetenzen

Kinder schützen heisst, sie auch in der digitalen Welt zu begleiten. Auf diesem Informationsportal erhalten Eltern, Lehr- und Betreuungspersonen Antworten, wie sie die Heranwachsenden im Medienalltag kompetent begleiten können – hin zu einer sicheren und altersgerechten Mediennutzung.

Mehr Informationen unter:
www.jugendundmedien.ch

«eBanking – aber sicher!»

Auf www.ebankingabersicher.ch finden Interessierte praxisnahe Informationen zu notwendigen Massnahmen und Verhaltensregeln für eine sichere Anwendung von E-Banking-Applikationen. Die Hochschule Luzern – Informatik wurde von führenden Schweizer Finanzinstituten mit dem Aufbau dieses Portals beauftragt, und es wird zurzeit von über 70 Finanzinstituten aus der ganzen Schweiz und aus dem Fürstentum Liechtenstein getragen.

Mehr Informationen unter:
www.ebankingabersicher.ch

Veranstaltungshinweis 2017

Die **3. Konferenz des Sicherheitsverbundes Schweiz** bietet Einblick in die Ergebnisse der Evaluation der Nationalen Strategie zum Schutz der Schweiz vor Cyberrisiken und Diskussionen über das weitere Vorgehen im Bereich Cybersicherheit und Cyberkriminalität.

Mehr Informationen unter:
www.svs.admin.ch

Schweizerische Kriminalprävention
Haus der Kantone
Speichergasse 6
Postfach
CH-3000 Bern 7

www.skppsc.ch

Herausgeberin und Bezugsquelle
Schweizerische Kriminalprävention SKP
info@skppsc.ch, Tel. +41 31 320 29 50

Verantwortlich		Martin Boess, Geschäftsleiter SKP
Redaktor		Wolfgang Wettstein, Zürich
Übersetzungen	**F**	ADC, Martigny
	I	Annie Schirrmeister, Massagno
Layout		Weber & Partner, Bern
Druck		Vetter Druck AG, Thun
Auflage		D: 1350 Ex. | F: 300 Ex. | I: 100 Ex.
Erscheinungsdatum		Ausgabe 4 | 2016, Dezember 2016

Das **SKP Info 4 | 2016** ist als PDF-Datei zu finden unter: www.skppsc.ch/skpinfo. Es erscheint auch in französischer und italienischer Sprache.

vectomart/123RF