Schweizerische Eidgenossenschaft
Confédération suisse
Confederazione Svizzera
Confederaziun svizra

Eidgenössisches Justiz- und Polizeidepartement EJPD
Bundesamt für Polizei fedpol

März 2015

Jahresbericht 2014

Koordinationsstelle zur Bekämpfung der Internetkriminalität KOBIK

Bundesamt für Polizei fedpol

Koordinationsstelle zur Bekämpfung der Internetkriminalität (KOBIK)
Nussbaumstrasse 29
3003 Bern

www.kobik.ch
www.cybercrime.ch

Veröffentlichung: 26. März 2015

Bildquellen: KOBIK, Thinkstock

Vorwort

von Herrn Regierungsrat Christoph Neuhaus,
Vorsitzender des Leitungsausschusses KOBIK

Panta Rhei, alles bleibt im Fluss – wie gewohnt schaut KOBIK nach vorne, muss sich laufend anpassen. Immer neue Herausforderungen, Erfahrungen sammeln, selbstkritisch analysieren und das Angebot ständig verbessern, das bleibt oberste Maxime.

Im Frühling wurde KOBIK von den deutschen Behörden über einen Fall von grossflächigem Identitätsdiebstahl informiert. Kriminelle versuchten, sich mittels E-Mail-Adressen und den zugehörigen Passwörtern in E-Mail-Konten einzuloggen und diese für den Versand von SPAM-Mails zu missbrauchen. KOBIK reagierte schnell und pragmatisch. Die Provider sowie über 38 000 Bürgerinnen und Bürger wurden bereits am nächsten Tag persönlich informiert. Die Reaktionen waren durchaus positiv und die nationale Koordinationsstelle zur Bekämpfung der Internetkriminalität bewies, wie schnell sie in der Lage ist, auf unerwartete Situationen zu reagieren.

KOBIK arbeitet proaktiv mit INTERPOL, Europol, dem FBI, HSI und vielen anderen ausländischen Behörden zusammen. Als Vertreterin der Schweiz ist KOBIK in internationalen Arbeitsgruppen mit den folgenden Partnern präsent: den Schweizer Staatsanwaltschaften, Kantonspolizeien, mit Vertretern der Finanzbranche, den Internet Service Providern oder mit der Melde- und Analysestelle Informationssicherung MELANI, mit SWITCH Internet Domains aber auch mit NGOs. Weitere Beteiligte sind die Schweizerische Kriminalprävention, der Nachrichtendienst des Bundes, das EDA und weiteren Bundes- und kantonalen Stellen. Damit die Schweiz auch in schwierigen Zeiten auf Unterstützung zählen darf, braucht es, wie alt-Bundesrat Ogi immer wieder herausstrich, die persönliche Kontaktpflege und Freundschaften auf internationaler Ebene.

Zu dieser internationalen Zusammenarbeit zählt die Zerschlagung von illegalen Botnetzen – das sind infizierte Computersysteme – wie auch die Koordination von Operationen zur Verhaftung von Hackern. Ebenso wichtig sind die Mitgliedschaft in internationalen Gremien zur Bekämpfung der Pädokriminalität im Internet oder Allianzen wie die der Global Alliance. Vor allem aber muss durch gute Arbeit immer wieder Vertrauen geschaffen werden. Damit bleibt KOBIK bei der Bekämpfung von Cyberkriminalität ein geschätzter und anerkannter Partner.

KOBIK wird sich auch inskünftig nicht über mangelnde Arbeit oder fehlende Herausforderungen beklagen müssen. Die virtuellen Banküberfälle mit Milliardenbeute, die Sicherstellung von Rekordmengen an kinderpornografischem Material oder Millionenschäden bei Schweizer KMUs wegen Social Engineering verdeutlichen, dass KOBIK (zu zwei Dritteln durch die Kantone und einem Drittel durch den Bund finanziert) mit zehn Mitarbeitenden und sechs zur Unterstützung zugewiesenen fedpol-Mitarbeitenden ausgelastet ist. Zudem legt KOBIK dem Bundesrat bis Ende 2016 das Konzept zur Umsetzung der Massnahme 6 der Nationalen Strategie zum Schutz der Schweiz vor Cyberrisiken (M6 NCS) vor. Diesbezüglich schreiten die Arbeiten zu einer Fallübersicht und der Koordination von interkantonalen Fallkomplexen voran.

KOBIK ist gefragt – kaum ein Tag vergeht, an dem nicht über einen neuen und noch grösseren Fall von Cyberkriminalität berichtet wird. Vielleicht liegt die grösste Herausforderung für KOBIK darin, den Entscheidungsträgern ein allgemeines und breites Verständnis für die Tragweite der Cyberkriminalität zu vermitteln? Es braucht gute Rahmenbedingungen und damit auch Investitionen in diese Sicherheit, selbst wenn das Ganze mit Kosten verbunden ist.

Inhaltsverzeichnis

1 Das Wichtigste in Kürze

- 2014 gingen bei KOBIK insgesamt 10 214 Meldungen über das Online-Meldeformular ein. Dies entspricht einer Zunahme von 10,9 Prozent gegenüber dem Vorjahr.
- 66,9 Prozent der Meldungen betrafen Vermögensdelikte. Diese haben im Verhältnis zu den strafbaren Handlungen gegen die sexuelle Integrität weiter zugenommen. Somit setzte sich der Trend der Vorjahre auch 2014 fort.
- Insgesamt 50 Meldungen führten direkt und aufgrund der strafrechtlichen Relevanz zur Übermittlung des Sachverhaltes an nationale und internationale Behörden und Organisationen.
- Durch aktive Recherchen in Peer-to-Peer-Netzwerken gelang es KOBIK im Berichtsjahr in 86 Fällen Internetanschlüsse zu identifizieren, die aktiv am Austausch von Kinderpornografie beteiligt waren.
- Verdeckte Vorermittlungen gemäss Polizeigesetzgebung des Kantons Schwyz und Verdeckte Ermittlungen nach Strafprozessordnung (StPO) durch KOBIK führten 2014 in insgesamt 29 Fällen zu Strafanzeigen zuhanden der zuständigen Kantone. 281 Fälle wurden zuständigkeitshalber an ausländische Strafverfolgungsbehörden zur Bearbeitung übermittelt.
- Mehr als tausend Meldungen im Zusammenhang mit strafrechtlich relevanten Internetseiten wurden via INTERPOL / Europol oder Organisationen mit verwandten Aufgaben (wie z. B. Inhope) an ausländische Behörden übermittelt.
- Die Umsetzungsarbeiten zur Massnahme 6 der Nationalen Strategie zum Schutz der Schweiz vor Cyberrisiken (NCS) sind im Gange.

2 KOBIK, die Meldestelle

Die nationale Koordinationsstelle zur Bekämpfung der Internetkriminalität (KOBIK) ist die zentrale Anlaufstelle für Personen, die verdächtige Internetinhalte melden möchten. Die Meldungen, welche über das Online-Meldeformular (www.cybercrime.ch) eingehen und strafrechtlich relevant sind, werden nach einer ersten Prüfung und Datensicherung an die zuständigen Strafverfolgungsbehörden im In- und Ausland weitergeleitet. Anfragen von Bürgerinnen und Bürgern versucht KOBIK soweit wie möglich direkt zu beantworten oder verweist die Betroffenen an die zuständigen Fachstellen oder an die lokal zuständigen Strafverfolgungsbehörden.

2.1 Meldungseingang

Im Zeitraum vom 1. Januar 2014 bis 31. Dezember 2014 sind bei KOBIK insgesamt 10 214 Verdachtsmeldungen und Anfragen über das Meldeformular auf www.cybercrime.ch eingegangen. Dies entspricht einer Zunahme von 10,9 Prozent im Vergleich zum Vorjahr (9208 Meldungen).

Die Anzahl der eingehenden Meldungen lässt keine gültigen Schlüsse auf das tatsächliche Ausmass der Internetkriminalität sowie der Zu- und Abnahme der illegalen Internetinhalte zu. Die folgenden Angaben widerspiegeln lediglich die Wahrnehmung der Gesellschaft von deliktischen Inhalten und Machenschaften im Bereich Internet sowie die Bereitschaft, diese aktiv bei der Polizei und weiteren Behörden zu melden.

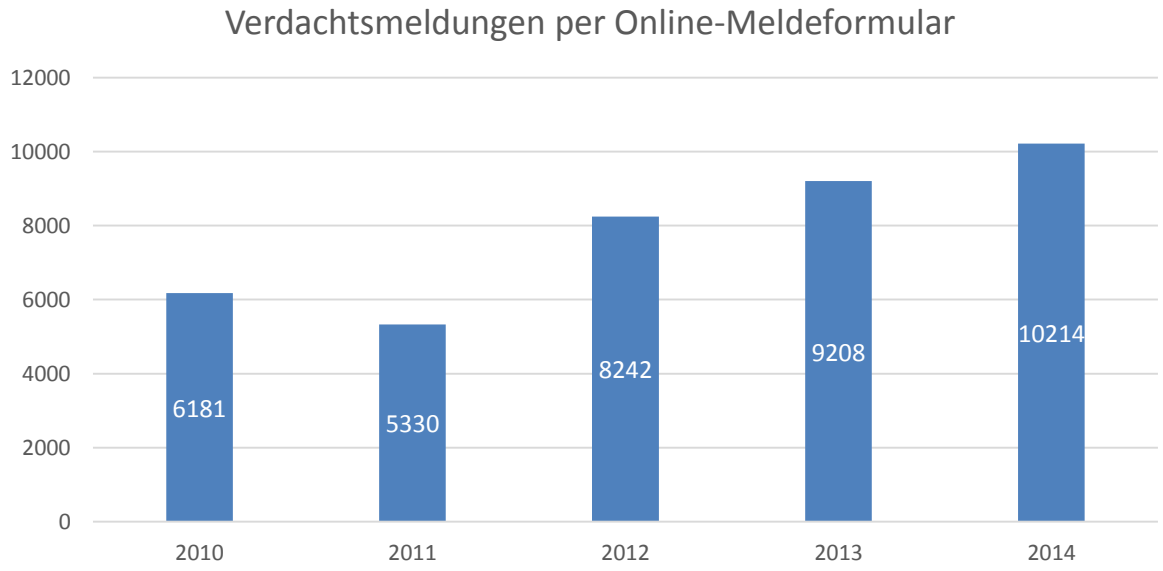


Abbildung 1: Meldungseingänge über www.cybercrime.ch im Jahresvergleich

Der Monatsdurchschnitt der Anzahl eingehender Meldungen liegt bei 851 Eingängen. Die bereits in den letzten zwei Berichtsjahren festgestellten Schwankungen im Mai (1024 Meldungen), Ende September (837 Meldungen) und zu Beginn Oktober (680 Meldungen) konnten auch dieses Jahr wieder beobachtet werden. Wie auch im letzten Jahr wurde im Mai eine erhöhte Anzahl Meldungen zu Phishing- und Betrugsversuchen und im September und Oktober eine entsprechende Abnahme registriert. KOBIK hat im Monat Mai aufgrund der Häufung der eingehenden Meldungen insgesamt vier Warnmeldungen zu den gemeldeten Phänomenen auf den Social-Media-Kanälen und der KOBIK-Webseite publiziert. Ein Grund für diese

Häufung könnte die von führenden Anti-Viren-Softwareherstellern festgestellte Fluktuation des Spam- und Phishing-Mail-Aufkommens im Zusammenhang mit der US-Amerikanischen Sommerferienzeit (Ende Mai bis Ende August) sein. Wie sich diese Effekte tatsächlich auf die Meldungseingänge auswirken, kann aber aufgrund der KOBIK zur Verfügung stehenden Daten nicht festgestellt werden.

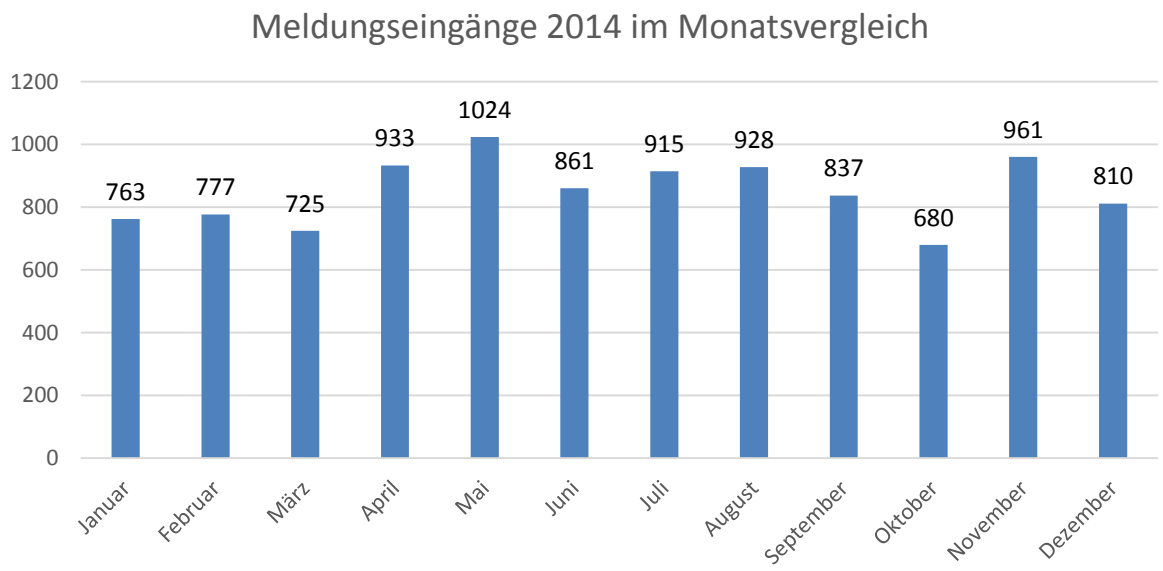


Abbildung 2: Meldungseingänge über www.cybercrime.ch im Monatsvergleich (Total: 10 214 Meldungen)

2.2 Was wurde gemeldet?

Die bei KOBIK gemeldeten Kriminalitätsformen lassen sich in zwei ineinander fliessende Bereiche aufteilen. Unter Internetkriminalität im engeren Sinne (IES) werden Straftaten verstanden, die mit Hilfe der Technologien des Internets verübt werden oder sich Schwachstellen dieser Technologien zu Nutze machen. Beispiele dafür sind Phänomene wie «Hacking», «Distributed Denial of Service» (DDoS) sowie das Herstellen und In-Umlauf-Bringen von Schadsoftware. Diese Straftaten wurden erst durch das Internet ermöglicht oder richten sich gezielt gegen dessen Technologien. Die Internetkriminalität im weiteren Sinne (IWS) nutzt das Internet als Kommunikationsmittel, wobei die sich bietenden Möglichkeiten wie beispielsweise der E-Mail-Verkehr oder der Austausch von Dateien für unlautere Zwecke missbraucht werden. Beispiele hierfür sind Betrugsmaschen auf Kleinanzeigeplattformen oder die Verbreitung von verbotener Pornografie.

Insgesamt wiesen 87,7 Prozent der eingegangenen Meldungen eine strafrechtliche Relevanz auf. Davon wurde wiederum bei 88,6 Prozent ein Bezug zum Strafgesetzbuch (StGB)[1] festgestellt. Die restlichen dieser Meldungen betrafen unter anderem Verstösse gegen das Bundesgesetz gegen den unlauteren Wettbewerb (UWG)[2], das Urheberrechtsgesetz (URG)[3], das

[1] Schweizerisches Strafgesetzbuch, vom 21. Dezember 1937, SR 311.0

[2] Bundesgesetz gegen den unlauteren Wettbewerb, vom 19. Dezember 1986, SR 241

[3] Bundesgesetz über das Urheberrecht und verwandte Schutzrechte, vom 9. Oktober 1992, SR 231.1

Markenschutzgesetz (MSchG)[4], das Betäubungsmittelgesetz (BetmG)[5] sowie das Geldwäschereigesetz (GwG)[6] (insgesamt 11,4 Prozent, siehe Kap. 2.2.3, Abbildung 9).

In rund 12 Prozent der Fälle konnte KOBIK nach einer Prüfung des Sachverhaltes keine strafrechtlich relevanten Inhalte feststellen. Diese Prozentzahl beinhaltet ebenfalls die Anfragen an KOBIK, die ohne einen Deliktshintergrund gestellt wurden.

Betraf der gemeldete Sachverhalt kein Offizialdelikt und bedurfte es daher einer Strafanzeige durch die Geschädigten, so verwies KOBIK die meldenden Personen an die hierfür zuständigen kantonalen Polizeistellen.

Der Anteil der Meldungen zu strafbaren Handlungen gegen das Vermögen ist im Vergleich zu den anderen strafrechtlich relevanten Meldungen erneut gestiegen. Insgesamt 6837 Meldungen (66,9 Prozent) betrafen diesen Deliktsbereich (Art. 137-172ter StGB). Mit 7,4 Prozent (758 Meldungen) an zweiter Stelle folgen Meldungen zu strafbaren Handlungen gegen die sexuelle Integrität (Art. 187-212 StGB). Im Vergleich zum Vorjahr hat sich die absolute Zahl dieser Meldungen wiederum massiv von 1842 auf 758 Meldungen (minus 58,8 Prozent) reduziert. Hierbei ist anzumerken, dass mit der am 1. Juli 2014 in Kraft getretenen StGB-Revision der Besitz und Vertrieb von harter Pornografie mit Exkrementen nicht mehr unter Strafe gestellt ist. Vergleiche hierzu auch Abschnitt 2.2.2.

[4] Bundesgesetz über den Schutz von Marken und Herkunftsangaben, vom 28. August 1992, SR 232.11

[5] Bundesgesetz über die Betäubungsmittel und psychotropen Stoffe, vom 3. Oktober 1951, SR 812.121

[6] Bundesgesetz über die Bekämpfung der Geldwäscherei und der Terrorismusfinanzierung im Finanzsektor, vom 10. Oktober 1997, SR 955.0

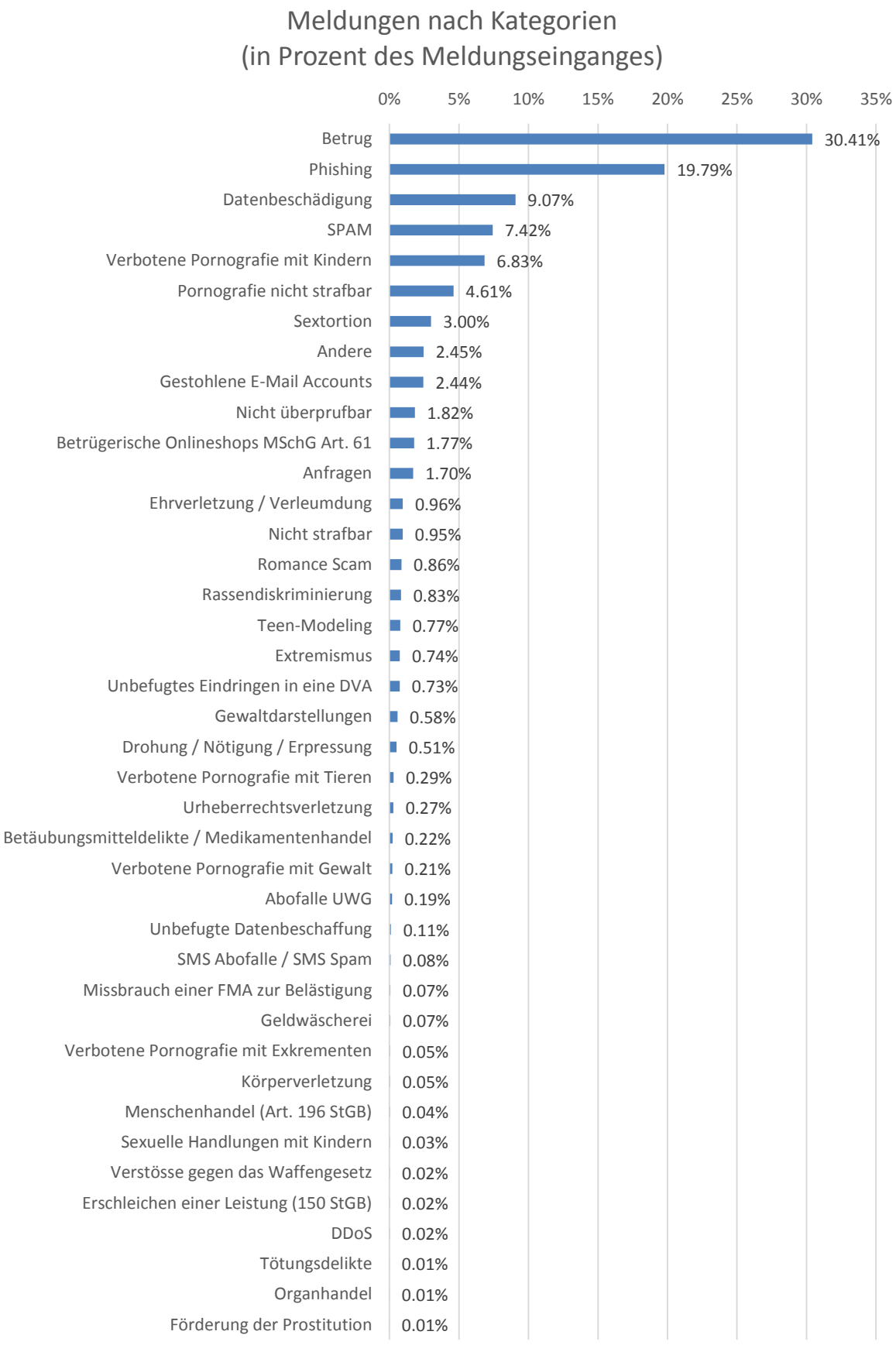


Abbildung 3: Prozentualer Anteil der Kategorien am Meldungseingang 2014 (Total: 10 214 Meldungen)

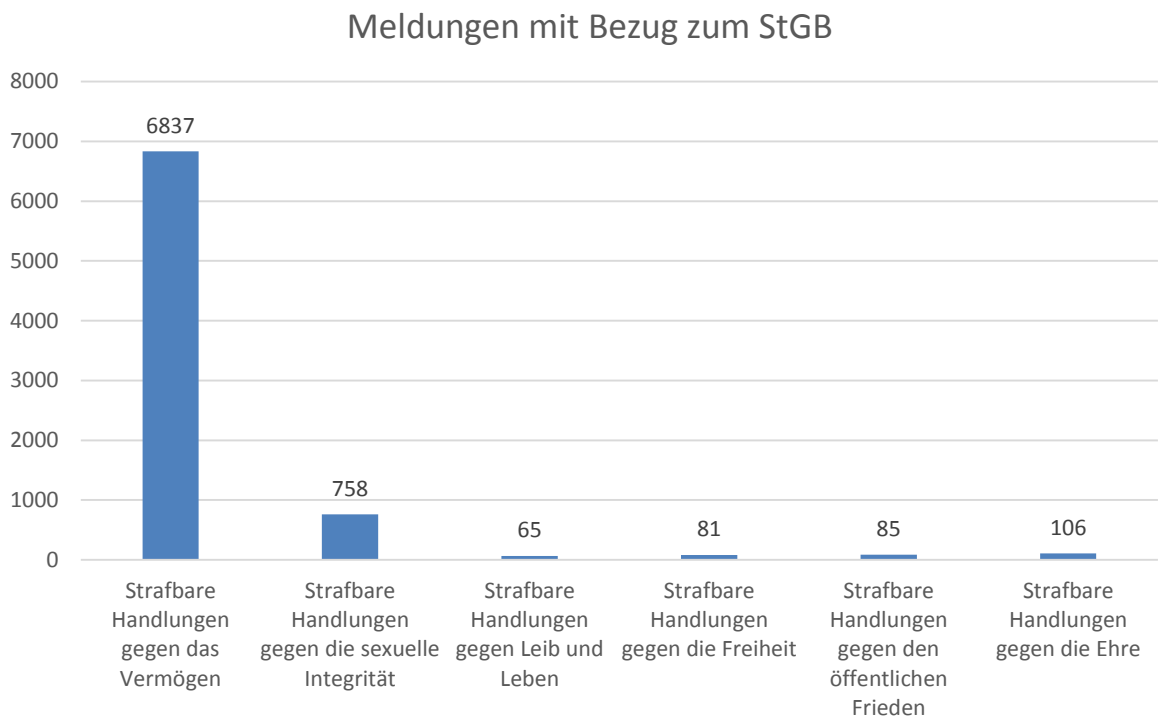


Abbildung 4: Meldungseingang 2014 mit Bezug zu unterschiedlichen Titeln des StGB (Total: 7932 Meldungen)

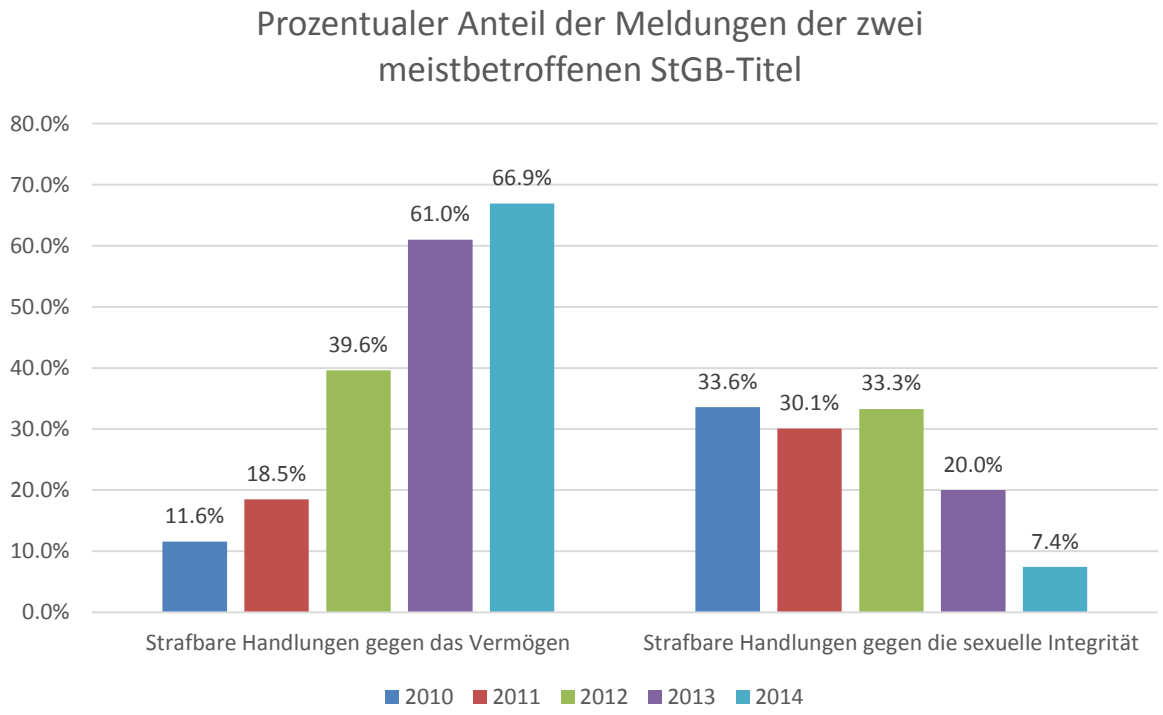


Abbildung 5: Entwicklung des prozentualen Anteils an Delikten zu StGB Titel 2 und 5, 2010 - 2014

2.2.1 Strafbare Handlungen gegen das Vermögen

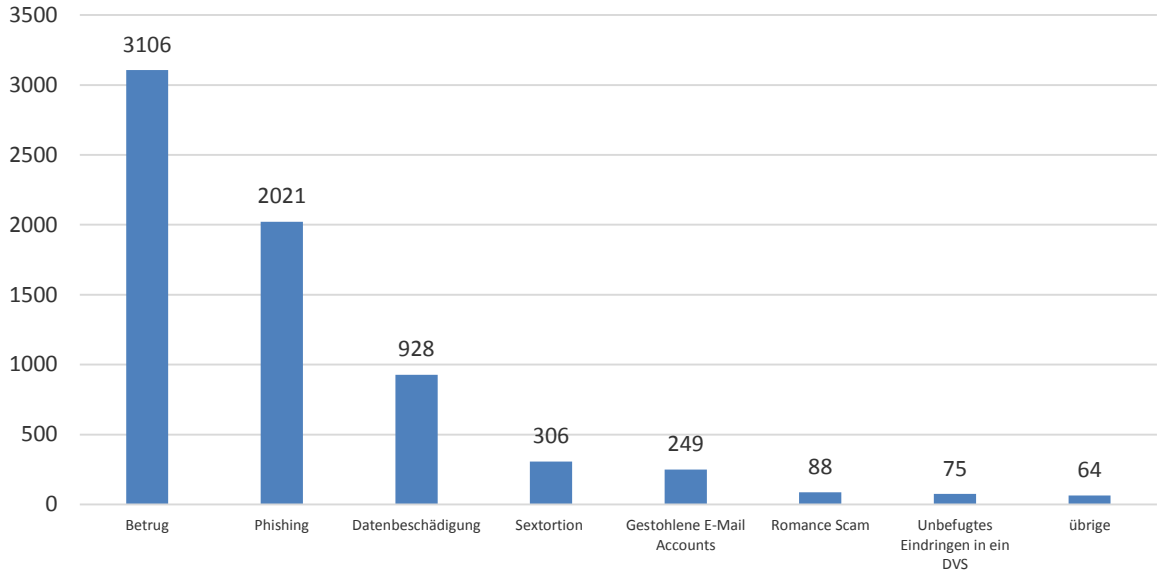


Abbildung 6: Meldungseingang zu strafbaren Handlungen gegen das Vermögen 2014 (Total: 6837 Meldungen)

66,9 Prozent (6837 Meldungen) des gesamten Meldungsvolumens betrafen strafbare Handlungen gegen das Vermögen. Die Zunahme scheint mit den Untersuchungsergebnissen von unabhängigen Quellen wie beispielsweise Quartalsreporte von Antiviren-Softwareherstellern oder Internet-Security-Forschern, zu korrelieren. Diese stellen fest, dass das Spam- und Phishing-Volumen sowie die Anzahl neu entdeckter Malware-Infektionen und Familien weltweit stetig zunehmen. Die untenstehende Auswahl an gemeldeten Vorgängen ist nicht vollständig, repräsentiert jedoch eine Vielzahl der eingegangen Verdachtsmeldungen.

2.2.1.1 Betrugsversuche (IWS)

Mit 30,4 Prozent der Anzahl an Eingängen (3106 Meldungen) machen Betrugsversuche den grössten Anteil des Meldungsvolumens aus. Im Vergleich zum Vorjahr wurden im Bereich der Internetkriminalität im weiteren Sinne keine allzu grossen Abweichungen von den bereits bekannten «Modi Operandi» festgestellt.

Viele der gemeldeten Betrugsversuche betrafen auch in diesem Berichtsjahr gefälschte Anzeigen auf Kleinanzeige- und Auktionsplattformen. Einerseits stehen die Kaufinteressenten im Visier. Die potentiellen Geschädigten werden durch besonders billige Angebote für allgemein begehrte Ware, wie beispielsweise Marken-Smartphones oder bestimmte Auto-Typen, zu äusserst günstigen Konditionen angelockt. Ziel der Betrüger ist es, aufgrund des tiefen Preises die Kaufinteressenten zu einer Vorschusszahlung zu bewegen, ohne dann aber die in Aussicht gestellte Ware zu liefern.

Ebenfalls häufig gemeldet wurden Betrugsversuche mit gefälschten Wohnungsinseraten. Bei dieser Masche nutzen die Betrüger die in den grösseren Schweizer Städten wie Zürich und Basel herrschende Wohnungsknappheit aus und erstellen Inserate für günstige, allerdings nicht existente Immobilien. Bei Vorauszahlung von bis zu drei angeblichen Monatsmieten als Kaution wird den Geschädigten versprochen, die Wohnung sofort beziehen zu können oder aber die Schlüssel für eine Besichtigung zugeschickt zu erhalten. Spätestens bei der ersten Besichtigung entpuppt sich das Schnäppchen an der nicht existenten Adresse als Betrug.

Andererseits sind aber nicht nur Käufer das Ziel für die Betrüger sondern auch Verkäufer und

Inserenten. Die Betrüger antworten zum Beispiel auf Anzeigen für Elektronikartikel und versuchen, die Verkäufer zu einem Versand der Ware ins Ausland zu überreden und sogar einen höheren Preis dafür zu bezahlen, als der Verkäufer ursprünglich verlangte. Oftmals wird versucht glaubhaft zu machen, dass gewisse in der Schweiz auf Kleinanzeigeplattformen erhältliche Elektronikartikel im Ausland nicht erstanden werden können. Die Täterschaft gibt vor, für eine Drittperson zu agieren, die nicht in der Schweiz wohnhaft sei und deshalb das Geschäft nicht selber abwickeln könne. Steigt der potentielle Geschädigte auf das Geschäft ein, wird dieser aufgefordert, die Ware zu versenden. Die abgemachte Summe trifft aber in der Regel nicht ein. Bei Varianten dieser Betrugsform versucht die Täterschaft, die Verkäufer zum Zahlungsempfang via Online-Zahlungsdienstleister zu überreden. Danach werden durch die Betrüger falsche Zahlungsbestätigungen für die gekaufte Ware an den Verkäufer versendet, die oftmals den tatsächlich geforderten Betrag übersteigen. Der Geschädigte wird dann in angeblich vom Zahlungsdienstleister stammenden E-Mails aufgefordert, Gebühren für anfallende Dienstleistungen wie Zoll, Verschiffungstarife und weitere zu bezahlen. Die Täterschaft begleitet die Geschädigten dabei fortlaufend via E-Mail und versichert, sämtliche Kosten zu übernehmen, um somit allfällig aufkeimenden Verdacht des Verkäufers zu beschwichtigen. In Wirklichkeit stammen sämtliche E-Mails des Zahlungsdienstleisters und dessen Forderungen von der Täterschaft selbst. Die bezahlten Beträge fliessen in die Taschen der Täter, dies oftmals zusätzlich zum Verlust der vermeintlich verkauften Ware.

Vermehrt geraten auch kleine und mittlere Unternehmen (KMU) ins Visier von Betrügern. Die Täterschaft betreibt einen beachtlichen Aufwand, um an Informationen über Zahlungsmodalitäten von Unternehmen zu gelangen. Beispielsweise informieren sich die Täter in einer ersten Phase über Personen in den Unternehmen, die regelmässigen Kontakt zu Treuhandbüros und Banken haben. Ebenso wird versucht, mittels der mit der Phishing-Methode gestohlenen E-Mail-Zugangsdaten an Informationen über Zahlungsmodalitäten und ausstehende Zahlungen zu gelangen. Die Täter setzen danach diese Erkenntnisse ein, um mittels gefälschten E-Mails an die Kundenberater der Banken oder Treuhandbüros der entsprechenden Firmen Zahlungen umzuleiten oder auszulösen. Die Masche kann höchst ertragreich sein; die so ergatterten Beträge reichen in den gemeldeten Fällen von einigen hundert bis zu mehreren zehntausend Franken. Aufgrund der von den kantonalen Polizeibehörden eingehenden Meldungen (vgl. Kapitel 4) wird die Gesamtschadenssumme in der Schweiz bereits auf mehrere Millionen Franken geschätzt.

2.2.1.2 Sextortion (IWS)

Erste Meldungen zum Phänomen «Sextortion» (Wortkombination aus «Sex» und «Extortion» englisch für Erpressung) erreichten KOBIK bereits im Berichtsjahr 2013. Bei dieser Masche gaben die meist männlichen Geschädigten an, dass diese von unbekannter, angeblich weiblicher Täterschaft auf Social-Media und Dating-Plattformen kontaktiert wurden. Im Anschluss wurde die Unterhaltung auf Video-Chat-Dienste verlagert. Daraufhin begann die Frau, sich vor der Kamera auszuziehen und verführte damit das Gegenüber zu sexuellen Handlungen vor laufender Kamera, welche heimlich mitgeschnitten wurden. Anschliessend drohte die Täterschaft in einer E-Mail, die kompromittierenden Aufnahmen zu veröffentlichen, sollte nicht ein entsprechendes Lösegeld bezahlt werden, welches sich in der Regel auf wenige hundert Franken belief. In den gemeldeten Fällen wurde auch trotz Bezahlung eines Lösegeldes das kompromittierende Video auf Social-Media Plattformen veröffentlicht. Zudem wurden die Zahlenden weiterhin erpresst und erhielten erneut Aufforderungen, zur Bezahlung von Lösegeldern in steigenden Beträgen.

2.2.1.3 Phishing (IWS / IES)

Mit insgesamt 2021 Meldungen (19,8 Prozent) ist die Anzahl der gemeldeten Phishing-Versuche (minus 8,5 Prozent) gegenüber dem Vorjahr (2208 Meldungen) leicht gesunken. Phishing-Versuche zielen darauf ab, via nicht zielgerichtetem Massenversand von E-Mails möglichst viele Personen auf Webseiten zu locken, die bekannten Internetdienstleistern nachempfunden sind. Auf diesen Webseiten werden dann die entsprechenden Personen dazu verleitet, Benutzernamen und Passwörter für die jeweiligen Dienstleistungen bekannt zu geben. Nicht nur E-Banking-Dienste und Online-Zahlungsdienstleister sind für die Täterschaft interessant, sondern auch Zugangsdaten für Auktions- und Einkaufsplattformen, Cloud-Speicherdienste, Musik-Download-Seiten und App-Stores für Smartphones.

Vielfach befanden sich die im Berichtsjahr gemeldeten Phishing-Seiten auf Servern von Drittpersonen, die von der Täterschaft missbraucht wurden. Beispielsweise wurden Sicherheitslücken in Content-Management-Systemen ausgenutzt, um eine Phishing-Seite auf dem dadurch verwundbaren Webserver zu platzieren. Auch der Versand der Phishing-Mails fand in einigen Fällen über auf ähnliche Weise missbrauchte Webserver oder mittels Bot-Netzen statt.

2.2.1.4 Police-Ransomware (IES)

Police-Ransomware (Kombination aus den englischen Wörtern «Ransom» für Lösegeld und «Malware» für Schadsoftware) bezeichnet eine Form von Schadsoftware, die den Computer für jegliche weitere Interaktion für den Benutzer sperrt und ein Lösegeld in der Höhe von wenigen hundert Franken zur Entsperrung fordert, zahlbar über einen anonymen Online-Zahlungsdienstleister. Der Geldforderung wird zusätzlich Druck verliehen, indem auf der angezeigten Sperrseite offizielle Logos von Polizeieinheiten und anderen staatlichen Organisationen angezeigt werden. Die betroffenen Computer infizieren sich beispielsweise durch das unbedachte Öffnen eines E-Mail-Anhangs oder den Besuch einer entsprechend präparierten Webseite. Die Verteilung dieser Schadsoftware ist nicht zielgerichtet. Ziel der Täterschaft ist es vielmehr, eine möglichst grosse Anzahl von Computern zu infizieren, um so den Gewinn aus der Masse der Infektionen zu maximieren. Im Unterschied zum nachfolgend erwähnten Verschlüsselungstrojaner stellt es für eine Fachperson einen relativ kleinen Aufwand dar, ein infiziertes System zu bereinigen und die darauf befindlichen Dateien wieder herzustellen.

2.2.1.5 Crypto-Ransomware (IES)

Bereits im zweiten Halbjahr 2013 begannen sich Meldungen über so genannte Verschlüsselungs-Trojaner (Crypto-Ransomware – Kombination aus Englisch «Cryptography» für Wissenschaft der Verschlüsselungstechniken und «Ransomware», also erpresserische Schadsoftware) zu häufen. Diese Art von Schadsoftware verteilt sich analog zu Police-Ransomware via E-Mail-Anhänge und präparierte Webseiten. Infiziert sich der Computer des Benutzers, so verschlüsselt die Software im Hintergrund sämtliche Dateien gängiger Anwendungsprogramme, beispielsweise durch Office-Lösungen erzeugte Dokumente oder Musik- und Video-Dateien. Diese werden somit für den Benutzer unbrauchbar gemacht und können im schlimmsten Fall auch von Fachpersonen gar nicht oder nur mit einem erheblichen Aufwand wiederhergestellt werden. Anschliessend wird der Benutzer über die Verschlüsselung informiert und aufgefordert, via virtuelle Währungen einen gewissen Betrag für die Entschlüsselung der Dateien zu bezahlen. Auch bei Bezahlung des geforderten Betrages besteht keinesfalls die Garantie, dass die Verschlüsselung von den Tätern rückgängig gemacht wird.

2.2.1.6 E-Banking-Trojaner und Key-Logger (IES)

Im laufenden Berichtsjahr wurden zahlreiche verdächtige E-Mails mit E-Banking-Schadsoftware im Anhang gemeldet. Der Nachrichtentext dieser E-Mails ist durch die Täterschaft so verfasst, dass dieser die Empfänger zum Öffnen des entsprechenden Anhangs und somit zur Installation der Schadsoftware bewegt. So steht beispielsweise im Nachrichtentext, dass sich im Anhang eine unbezahlte Rechnung eines grossen Online-Versandhauses befindet. In anderen Fällen gibt der Inhalt vor, dass sich im Anhang eine Auflistung von Mobiltelefon-Auslandsgesprächen befinde. Einmal installiert, ist die Schadsoftware in der Lage, in vom Benutzer geöffnete E-Banking-Sitzungen einzudringen und die angezeigten Browserinhalte abzuändern. Für den Benutzer sieht es so aus, als würden gerade Wartungsarbeiten durchgeführt. Tatsächlich aber werden im Hintergrund Transaktionen getätigt. Des Weiteren sind die verschiedenen Schadsoftwarevarianten in der Lage, Tastatureingaben und Netzwerkverkehr aufzuzeichnen, so dass Benutzernamen und Passwörter von der Täterschaft gestohlen werden können.

2.2.2 Strafbare Handlungen gegen die sexuelle Integrität

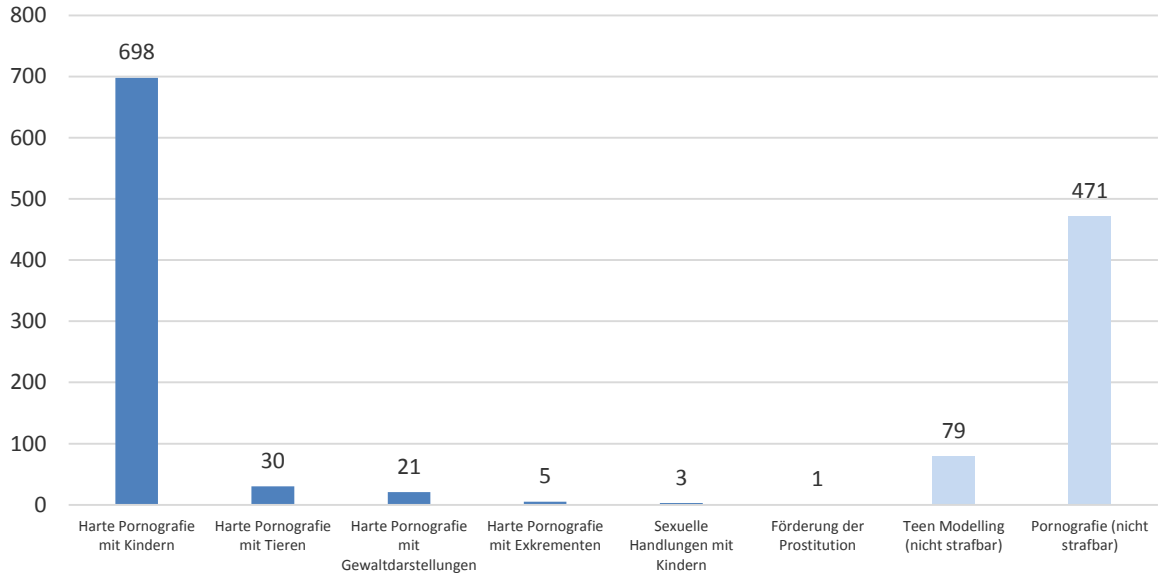


Abbildung 7: Meldungseingang zu strafbaren Handlungen gegen die sexuelle Integrität 2014 (Total: 758 Meldungen)

Die Anzahl der Meldungen zu Delikten gegen die sexuelle Integrität hat im Berichtsjahr erneut deutlich abgenommen. Die Zahl der Meldungen sank um fast 58,8 Prozent gegenüber dem Vorjahr von 1842 auf 758.

Die Anzahl der gemeldeten Webseiten, welche verbotene Pornografie mit Kindern anbieten, ist erneut deutlich von 1414 Meldungen im Vorjahr auf 698 Meldungen (minus 50,6 Prozent) gesunken. Zu beachten ist, dass seit dem 1. Juli 2014 eine Gesetzesänderung in Kraft ist, welche das Verbot der Herstellung und Vertrieb der Pornografie mit Exkrementen aufhebt. Dies hat zur Folge, dass Meldungen, die ab dem 1. Juli 2014 eingegangen sind, als nicht mehr strafrechtlich relevant galten und somit den Meldungen zu nicht strafbaren Inhalten zugeteilt wurden.

Zusätzlich gingen bei KOBIK insgesamt 79 Verdachtsmeldungen zu Webseiten, welche so genannte Teen-Modeling-Bilder als Inhalt haben. Diese Inhalte sind nicht pornografischer Natur im Sinne des Strafgesetzbuches und somit nicht strafrechtlich relevant. Die Bilder zeigen

beispielsweise Teenager in aufreizender Pose oder in nicht altersgerechter, das heisst unangepasst freizügiger oder aufreizender Kleidung. Obwohl diese Erzeugnisse nicht als Kinderpornografie im strafrechtlichen Sinne gelten, werden sie oftmals von Internet-Nutzern als kinderpornografisch empfunden und deshalb KOBIK gemeldet.

In weiteren 471 Fällen wurde KOBIK auf Inhalte aufmerksam gemacht, bei denen sich nach einer genaueren Prüfung keine strafrechtliche Relevanz ergab, die jedoch bei KOBIK durch die Melder als vermeintlich verbotene Pornografie gemeldet wurden. Hierbei handelt es sich beispielsweise um Webseiten mit Pornografie mit Ausscheidungen (seit 1. Juli keine strafrechtliche Relevanz mehr) oder Webseiten, die aufgrund der dargestellten Sexualpraktiken von den Meldern als anstössig empfunden werden, die jedoch keine strafrechtliche Relevanz aufweisen. Somit sind diese nicht in der Statistik der strafrechtlich relevanten Delikte gegen sexuelle Integrität aufgeführt.

Der Rückgang der Meldungen zu Delikten gegen die sexuelle Integrität erklärt sich aus Sicht KOBIK einerseits aufgrund der gesteigerten Effizienz bei der Bearbeitung der Sperrliste durch KOBIK und durch die gute Zusammenarbeit mit den Internet Service Providern (ISPs) und INTERPOL. KOBIK leistet dabei einen bedeutenden Beitrag zur Erstellung der Worst of Liste (IWOL) von INTERPOL (vgl. hierzu Kapitel 6). Durch die Zusammenarbeit vieler Suchmaschinenanbieter wie Google und Microsoft mit INTERPOL können viele Seiten gar nicht mehr über die Suchmaschinen gefunden werden. KOBIK geht davon aus, dass diese Zusammenarbeit und die gesteigerte Effizienz mit der Sperrliste bei der Zusammenarbeit mit den Providern ein Grund für den Meldungsrückgang solcher Seiten sein könnte, da entsprechend weniger Bürgerinnen und Bürger mit solchen Angeboten konfrontiert werden. Durch die proaktive Zusammenarbeit mit INTERPOL zur Erstellung der IWOL aber auch mit den Schweizer ISPs leistet KOBIK einen wichtigen Beitrag zur Senkung der Verfügbarkeit von verbotenem Bildmaterial im Internet und somit der Reviktimisierung von Opfern durch wiederholten Konsum ihrer bildlich festgehaltenen Missbräuche durch Konsumenten verbotener Pornographie.

Andererseits könnte der Meldungsrückgang mit den bereits seit 2012 festgestellten Tendenzen zusammen hängen, dass verbotene pornografische Inhalte einerseits in nicht öffentlich einsehbaren Bereichen des Internets, beispielsweise The Onion Router (TOR)-Netzwerk oder Invisible-Internet-Project (I2P), ausgetauscht werden oder die Täterschaft auf Private-Peer-to-Peer-Lösungen (siehe Kap. 3.2) ausweicht.

2.2.3 Weitere strafbare Handlungen

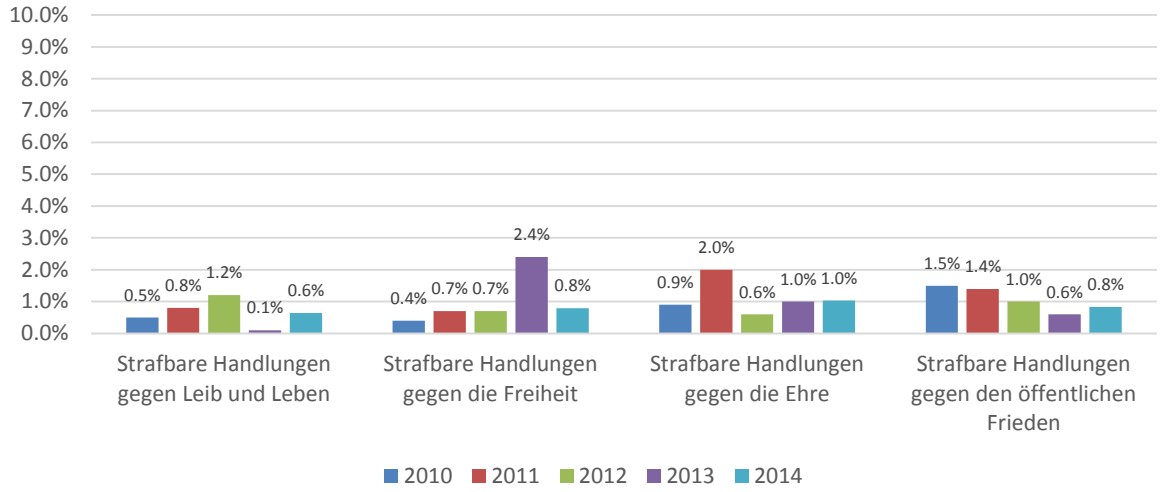


Abbildung 8: Meldungseingang 2010 - 2014 zu weiteren StGB-Titeln im Vergleich (prozentualer Anteil aller Meldungen)

3,3 Prozent des Meldeaufkommens betraf die übrigen StGB-Titel der strafbaren Handlungen gegen Leib und Leben, die Freiheit, den öffentlichen Frieden und die Ehre. Zu strafbaren Handlungen gegen den öffentlichen Frieden wurden 85 Meldungen registriert. Diese betrafen mehrheitlich diskriminierende oder extremistische Äusserungen auf Social-Media Plattformen. Zwar bleibt der relative Anteil Meldungen zu diesen Themen auf dem gleichen Stand wie in den letzten Jahren, trotzdem gibt es eine leichte Zunahme der absoluten Anzahl.

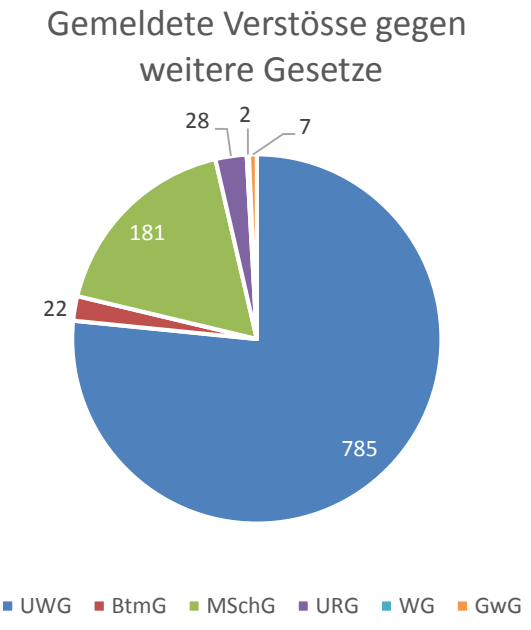


Abbildung 9: Aufteilung der 2014 gemeldeten Verstösse gegen weitere Gesetze (insgesamt 10,0 Prozent des totalen Meldevolumens

In 10,0 Prozent der Meldungen wurde ein Bezug zu weiteren Gesetzen festgestellt. Weitaus am häufigsten betroffen war das UWG, das sämtliche Meldungen zu unerwünschten Werbe-E-Mails (Spam) beinhaltet.

Im Berichtsjahr wurde insgesamt 181 Mal auf möglicherweise betrügerische Online-Shops und Produktpiraterie auf gefälschten Seiten von Markenartikelherstellern aufmerksam gemacht. Hierbei handelt es sich in den meisten Fällen um Online-Shops, die sich als Discounter für Luxus-Artikel und Markenwaren (Sportartikel, Sonnenbrillen, Designer-Taschen und weitere) ausgeben. Wird Ware zu gegenüber den Herstellerangaben massiv verbilligten Preisen auf diesen Webseiten bestellt, so werden entweder gar keine Waren geliefert oder aber Fälschungen in sehr niedriger Qualität. In insgesamt 76 Fällen waren solche betrügerische Onlineshops unter einem .ch Domain-Namen abrufbar.

Das Entfernen solcher Inhalte ausserhalb eines laufenden Strafverfahrens ist sehr zeitaufwändig. KOBIK muss im Verdachtsfall zu diesem Zweck die Registrierungsstelle SWITCH um eine gültige Schweizer Adresse des Domaininhabers anfragen lassen. Nur dank den allgemeinen Geschäftsbedingungen von SWITCH besteht die Möglichkeit, nach einer Wartefrist von 30 Tagen den entsprechenden Domain-Namen durch SWITCH löschen zu lassen, da die Inhaber in den meisten Fällen einer solchen Aufforderung nicht nachkommen.

2.2.4 Zusammenfassung

Der Anteil und die Gesamtanzahl an Meldungen zu Delikten gegen das Vermögen ist auch 2014 weiter gestiegen. Damit bestätigt sich der Trend der Vorjahre. Gleichzeitig ist die Anzahl der Meldungen zu Delikten gegen die sexuelle Integrität (ebenfalls gemäss den Vorjahrestrends) zurückgegangen. Die Anzahl der Meldungen zu den übrigen Titeln des Strafgesetzbuches und weitere strafrechtlich relevante Inhalte machen einen gleichbleibenden Anteil aus.

Grundsätzlich sind die 2014 festgestellten Phänomene nicht neu, sondern entsprechen in leicht abgeänderter Form den in den Vorjahren festgestellten Modi Operandi. Feststellbar ist aber eine Zunahme der Qualität der deliktischen Inhalte. Grammatik und Rechtschreibung von entsprechenden E-Mails, beispielsweise bei Phishing oder für Kleinanzeigen, werden fortlaufend verbessert. Ebenso wird die optische Aufmachung von Inseraten, Phishing-Seiten und E-Mails zunehmend professioneller, sodass es für den Benutzer schwieriger wird, zwischen einer echten Webseite und einer Nachahmung zu unterscheiden.

2.3 Produkte

KOBIK führt aufgrund der über das Meldeformular eingehenden Meldungen diverse Arbeiten aus und trifft Massnahmen zur Entfernung/Löschung der strafbaren Inhalte oder leitet die Meldungen an die zuständigen Strafverfolgungsbehörden weiter.

- Insgesamt 10 214 Meldungen wurden auf allfällige strafrechtliche Relevanz geprüft und beurteilt.
- In 3218 von 10 214 Fällen wurden die Meldenden mit einer persönlichen Antwort bedient.
- 50 Meldungen führten direkt und aufgrund der strafrechtlichen Relevanz zur Übermittlung des Sachverhaltes an den zuständigen Kanton oder an die zuständige Behörde.
- Mehr als tausend Meldungen im Zusammenhang mit strafrechtlich relevanten Internetseiten wurden via INTERPOL / Europol oder Organisationen mit verwandten Aufgaben (wie z. B. Inhope) an ausländische Behörden übermittelt.
- Zahlreiche Meldungen führten zu fedpol-internen Hinweisen an die Kommissariate Allgemeine-, Organisierte- und Finanzkriminalität sowie Pädokriminalität und Pornografie der Bundeskriminalpolizei und der Meldestelle für Geldwäscherei MROS.
- Häufig gemeldete Sachverhalte führten zur Veröffentlichung von insgesamt 27 Warnmeldungen auf der KOBIK-Webseite www.cybercrime.ch. Diese werden seit Ende 2013 auch auf den Social-Media-Plattformen Facebook und Twitter von KOBIK publiziert. Zudem werden die Partnerorganisationen Melde- und Analysestelle Informationssicherheit (MELANI), die Schweizerische Kriminalprävention (SKP) aber auch die Medien direkt benachrichtigt. Damit können breite Teile der Öffentlichkeit über aktuelle Gefahren erreicht werden.

2.4 Ausgewählte Fallbeispiele

KOBIK wurde auf Videos auf einer Pornografie-Videoplattform aufmerksam gemacht, auf der ein Benutzer Videos von Gästen einer Schweizer Badeanstalt veröffentlichte. Die Aufnahmen wurden offensichtlich von den abgebildeten, zumeist weiblichen Personen ohne deren Erlaubnis erstellt. Oftmals wurde in den Videos auf die Brüste und Hinterteile der abgebildeten jungen Frauen fokussiert. Zudem wiesen die Videos Titel und Beschreibungen mit ehrverletzenden und sexistischen Äusserungen auf. Aufgrund der Einschaltung der Medien durch eine Geschädigte gingen folglich bei der lokal zuständigen Kantonspolizei mehrere Anzeigen wegen Ehrverletzungsdelikten ein. Dank der Unterstützung durch KOBIK gelang es der zuständigen Kantonspolizei, den Hersteller und Profilbesitzer in Zusammenarbeit mit den Plattformbetreibern zu identifizieren und den Täter festzunehmen.

Aufgrund der eingehenden Bürgermeldungen ist KOBIK in der Lage, Warnmeldungen zu verfassen und auf der Webseite sowie den Social-Media-Kanälen zu publizieren und damit eine präventive Wirkung zu erzielen. Ein Beispiel dafür ereignete sich im April, als sich Benutzer einer Social Media Plattform an KOBIK wandten. Diese hatten über die Plattform eine Anzeige für einen Wettbewerb erhalten, bei dem angeblich ein Auto zu gewinnen war. Die Anzeige gab vor, dass der Wettbewerb von der französischen und schweizerischen Vertretung der Herstellerfirma aus organisiert wurde. Alles, was die Teilnahme erforderte, war die Angabe der Telefonnummer. In Wirklichkeit aber verbarg sich hinter der gefälschten Anzeige eine Abofalle – die Angabe der Handynummer auf der Seite des Wettbewerbes führte zum Abschluss eines Abos für einen gebührenpflichtigen Mobildienst. Innerhalb einer Stunde nach Eingang einer Beschwerde eines Bürgers über das Meldeformular publizierte KOBIK bereits eine Warnung auf den Social-Media-Kanälen, die von verschiedenen nationalen und internationalen Medien und der Schweizerischen Kriminalprävention aufgegriffen und weiterverbreitet wurde.

3 Aktive Recherchen durch KOBIK

Jedes Jahr wird durch den Leitungsausschuss KOBIK festgelegt, in welchen Bereichen der Internetkriminalität der Schwerpunkt der aktiven Recherchen gesetzt wird. Wie in den letzten Jahren wurde dieser auch für das Jahr 2014 auf die Bekämpfung der Pädokriminalität im Internet gesetzt. Jedoch wurde aufgrund der seit 2012 stark steigenden Anzahl an Delikten gegen das Vermögen erneut festgehalten, dass KOBIK auch Ermittlungen bei Delikten gegen das Vermögen unternehmen soll. Dies wirkt sich insbesondere auf die Koordinationstätigkeiten von KOBIK (siehe Kapitel 4) aus, die sich grösstenteils auf die Sicherstellung des Informationsflusses bei Operationen zwischen in- und ausländischen Stellen beziehen.

Aufgrund der aktiven Recherchen wurden 2014 insgesamt 396 Anzeigen erstellt und an die zuständigen Behörden im In- und Ausland übermittelt. Dies entspricht einer leichten Abnahme von 6,4 Prozent gegenüber dem Vorjahr.

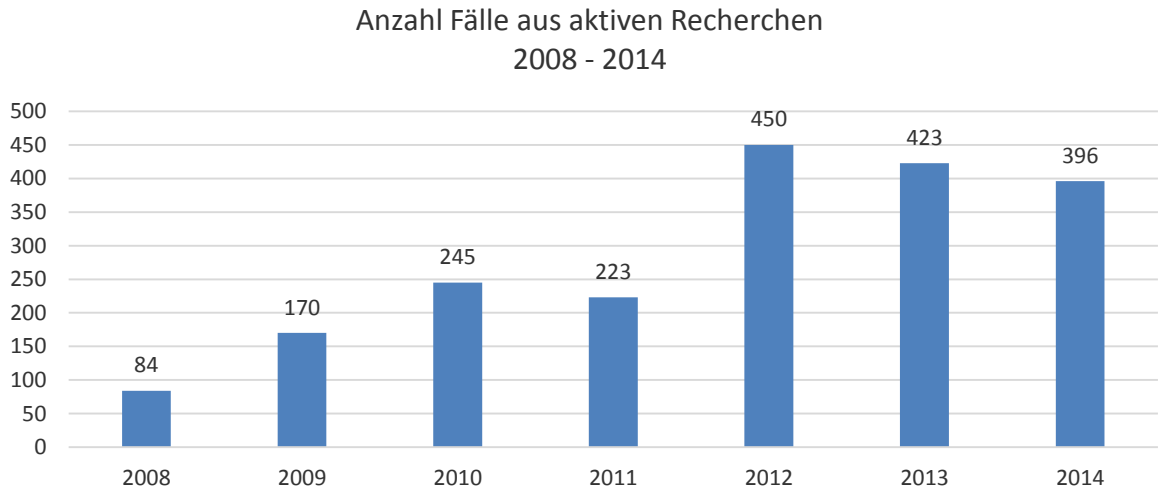


Abbildung 10: Im Rahmen aktiver Recherchen übermittelte Anzeigen (2008 – 2014)

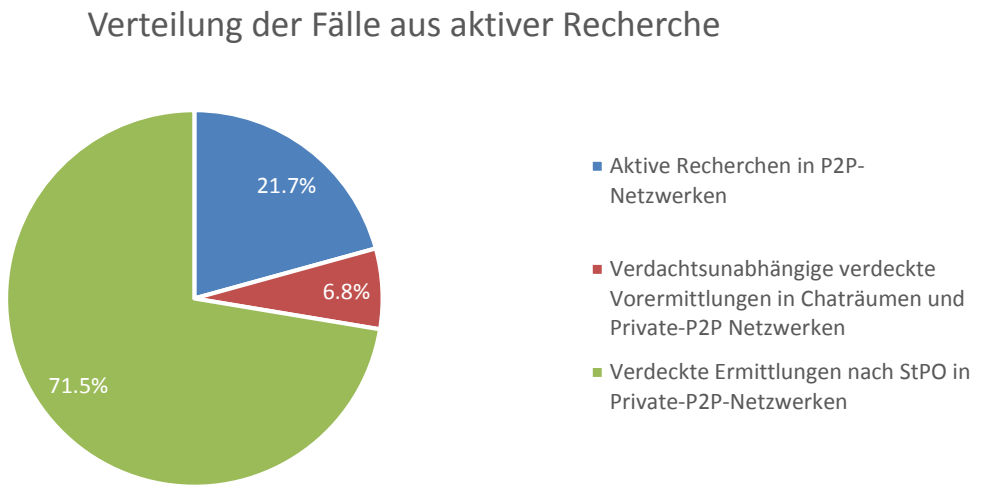


Abbildung 11: Herkunft der Strafanzeigen aus aktiver Recherche 2014 (Total: 396)

3.1 Aktive Recherchen in Peer-to-Peer-Netzwerken (P2P)

86 der 396 Anzeigen resultierten aus den aktiven Recherchen von KOBIK in öffentlich einsehbaren Peer-to-Peer-Netzwerken. Die Anzahl der gemeldeten Fälle ist im Vergleich zum Vorjahr erneut leicht gesunken. Dies ist unter anderem auch darauf zurück zu führen, dass die Zahl der Nutzer in den beobachteten Peer-to-Peer-Netzwerken in den letzten Jahren ebenfalls rückläufig ist und eine Verlagerung der Aktivitäten der Täterschaft in weniger einsehbare Bereiche des Internets wie in Private Peer-to-Peer (Private P2P) Netzwerke oder das Deep Web und Darknet[7] stattgefunden hat.

Die Dossiers richten sich gegen Internetnutzer, die aktiv und wiederholt harte Pornografie mit Kindern gemäss Art. 197 Abs. 4 oder Abs. 5 StGB austauschen. Obwohl KOBIK spezifisch nach Benutzern aus der Schweiz sucht, wurden im Berichtsjahr auch Straftaten von einer Person aus dem Ausland (USA) registriert. In solchen Fällen leitet KOBIK die Erkenntnisse an die zuständigen INTERPOL-Stellen im Ausland weiter.

3.2 Verdachtsunabhängige verdeckte Vorermittlungen

Die «Vereinbarung betreffend Zusammenarbeit bei den polizeilichen Vorermittlungen im Internet zur Bekämpfung der Internetkriminalität (Monitoring von Chat-Räumen)» zwischen KOBIK, dem Sicherheitsdepartement des Kantons Schwyz und dem Bundesamt für Polizei fedpol regelt die Modalitäten des Einsatzes von KOBIK-Mitarbeitern als verdeckte Vorermittler zur Bekämpfung der Pädokriminalität im Internet[8]. In diesem Sinne üben die Mitarbeitenden von KOBIK die verdeckte Vorermittlung ausschliesslich im Auftrag und unter Kontrolle der Kantonspolizei Schwyz aus. Damit ist gewährleistet, dass das Monitoring im Bereich Pädokriminalität im Internet auch im Sinne präventiver verdeckter Vorermittlungen im Internet neben den Kantonen weiterhin durch eine zentrale Stelle auf nationaler Ebene vorgenommen und die Bemühungen der einzelnen Kantone koordiniert werden können.

Verdeckte Vorermittlungen durch KOBIK führten 2014 in insgesamt 26 Fällen zu Strafanzeigen zuhanden der zuständigen Kantone und in einem Fall in das Ausland. Zwei Strafanzeigen basieren auf Vorermittlungen in speziell für Kinder vorgesehenen Chaträumen. In einem weiteren Fall wurde eine Anzeige erstellt, nachdem durch den Täter unaufgefordert die Webcam in einem Video-Chat eingeschaltet wurde und dadurch den verdeckten Vorermittler, der sich als minderjähriges Mädchen ausgab, in seine sexuellen Handlungen mit einbezog. In allen drei Fällen lautete die Anzeige auf versuchte sexuelle Handlungen mit Kindern nach Art. 187 StGB. Die tiefe Zahl der von KOBIK getätigten Ermittlungen in für Kinder vorgesehenen Chaträumen, hängt mit dem Umstand zusammen, dass die meisten Kantone nun über die gesetzlichen Grundlagen verfügen, um selber in solchen Chaträumen zu agieren. KOBIK stellt den kantonalen Polizeikorps eine zentrale Plattform zur nationalen Einsatzplanung und zum Informationsaustausch zur Verfügung. Diese soll verhindern, dass zwei Kantone gleichzeitig im selben Chatraum patrouillieren. Damit wurde ein Instrument für eine ständige und sich selbst organisierende interkantonale «Patrouillentätigkeit» im Netz auf nationaler Ebene geschaffen. Die Intensität dieser Patrouillentätigkeit hängt von den Möglichkeiten und Ressourcen der Kantone zur Vornahme von präventiven verdeckten Vorermittlungen für Fälle mit ausschliesslichem Bezug zur Schweiz ab.

---

[7] Ursprünglich bezeichnete der Ausdruck ein virtuelles Peer-to-Peer-Netzwerk, über das sich Nutzer nur gezielt mit Personen ihres Vertrauens austauschen. Mittlerweile versteht man unter Darknet das versteckte Web oder Deep Web, den Teil des World Wide Webs, der bei einer Recherche über normale Suchmaschinen nicht auffindbar ist.

[8] Einsatz im Sinne von § 9d des Gesetztes des Kantons Schwyz über die Kantonspolizei vom 22.03.2000 (PolG – SRZS 520.110)

Im Gegenzug konzentrierte KOBIK den Einsatz ihrer Ressourcen auf das Monitoring und die damit verbundenen verdeckten Vorermittlungen in privaten P2P Tauschbörsen, die zwingend zentral vorgenommen werden müssen sowie Einsätze im Darknet. In diesen Bereichen ist es anfangs ungewiss, woher Täter und Opfer stammen. Die geografische Verantwortlichkeit für die Strafverfolgung ist damit unklar. Aus ethisch-moralischer Sicht erscheint es im Sinne einer Notstandshilfe zwingend, dass solche Ermittlungen trotzdem durchgeführt werden, bis Opfer und/oder der Täter identifiziert bzw. lokalisiert und die Erkenntnisse den zuständigen Behörden übergeben werden können. KOBIK führt daher, stellvertretend für die Kantone, diese Ermittlungen an zentraler Stelle.

Die verbleibenden 24 Fälle beruhen auf verdeckten Vorermittlungen in sogenannten «privaten Peer-to-Peer-Tauschbörsen» (Private-P2P). Im Gegensatz zu den klassischen P2P-Netzwerken findet der Austausch der Dateien über eine öffentlich nicht einsehbare, verschlüsselte Direktverbindung zwischen den beteiligten Computern statt. Eine Kontaktaufnahme mit den Tätern bedingt daher den Einsatz verdeckter Vorermittler. Die meisten Anzeigen bei dieser Art der Ermittlungen lauteten auf den Besitz und die Verbreitung von verbotener Pornografie gemäss Art. 197 Abs. 4 oder Abs. 5 StGB, resp. Art. 197 Ziff. 3 oder Ziff. 3bis vor Inkrafttreten der Gesetzesrevision vom 1. Juli 2014.

3.3 Verdeckte Ermittlungen nach Strafprozessordnung

KOBIK wurde wie im Vorjahr auch 2014 von kantonalen Staatsanwaltschaften beauftragt, als direkt unterstellte Behörde verdeckte Ermittlungen in kantonal geführten Verfahren und damit gestützt auf die Strafprozessordnung (StPO) durchzuführen. Verdeckte Ermittlungen gemäss Art. 285a ff. StPO fanden ausschliesslich in privaten P2P-Tauschbörsen statt. Die Anordnungen basierten auf Strafverfahren, die aufgrund der von KOBIK durchgeführten verdachtslosen verdeckten Vorermittlungen nach Schwyzer Polizeigesetz eröffnet wurden und in denen sich im Verlaufe des Verfahrens neue Verdachtsfälle ergeben hatten. Aufgrund dieser Ermittlungen erstellte KOBIK insgesamt 283 Anzeigen.

Die von der private-P2P Community eingesetzte Software ermöglicht es, unabhängig vom Standort der beteiligten Benutzer direkte Verbindungen zwischen zwei Computern aufzubauen, um Dateien auszutauschen. Aufgrund dieser technischen Begebenheiten ist eine Fokussierung auf Schweizer Straftäter in solchen Fällen schwierig. Im Rahmen der angeordneten Ermittlungen wurden insgesamt drei Schweizer Benutzer identifiziert. Die restlichen 280 Anzeigen wurden zusammen mit den belastenden Beweisen im Rahmen des internationalen polizeilichen Informationsaustausches an die zuständigen ausländischen Strafverfolgungsbehörden übermittelt. Mit der systematischen Bearbeitung von Verdachtsmomenten, unabhängig der Täter- bzw. Opferherkunft, kommt KOBIK stellvertretend für die Kantone den Verpflichtungen der Schweiz aus der Global Alliance nach, indem weltweit gemeinsam und solidarisch gegen den Kindsmissbrauch im Internet vorgegangen wird. Die Kantone werden somit entlastet und müssen nicht Ressourcen zur Bearbeitung von Fällen aufwenden, deren Täterschaft schliesslich im Ausland zur Anzeige gebracht wird.

3.4 Rückmeldungen aus den Kantonen

Um eine Gesamtübersicht über die in den Kantonen eingeleiteten Massnahmen zu gewinnen, ersucht KOBIK die Kantone um Informationen über den weiteren Verlauf der ihnen angezeigten Verdachtsfälle (eingeleitete polizeiliche Massnahmen und/oder Ausgang des Gerichtsverfahrens).

Nachfolgend werden die im Berichtsjahr eingegangenen Rückmeldungen aus den Kantonen aufgelistet. Die grosse Mehrheit der angezeigten Fälle resultiert aus bereits in 2013 getätigten Recherchen, da die Rückmeldungen zu einem Grossteil erst nach Abschluss der entsprechenden Verfahren und nach Eintreten der Rechtskraft der Urteile zugestellt werden.

3.4.1 Rückmeldungen der kantonalen Polizeibehörden

Zum ersten Mal in der Geschichte von KOBIK wurde aufgrund der eingegangenen Rückmeldungen festgestellt, dass bei jeder von KOBIK ausgegangenen Verdachtsmeldung eine Hausdurchsuchung durchgeführt wurde.

Dies bedeutet jedoch nicht, dass in tatsächlich 100 Prozent der versendeten Dossiers eine Hausdurchsuchung stattgefunden hat oder stattfinden wird. Da noch nicht alle Feedback-Formulare für das Jahr 2013/14 eingegangen sind, ist die tatsächliche Anzahl der durchgeführten Hausdurchsuchungen nicht ermittelbar. Die hohe Rate an Hausdurchsuchungen zeigt jedoch, dass die Polizeikorps sich aktiv mit den KOBIK-Anzeigen auseinandersetzen und dass ihnen eine hohe Priorität zugewiesen wird.

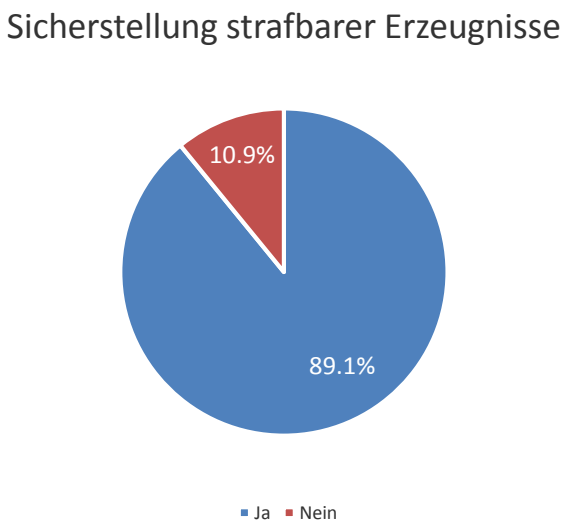


Abbildung 12: Prozentsatz der 2014 erfolgreichen Hausdurchsuchungen (Sicherstellung von strafbaren Erzeugnissen aufgrund einer Anzeige durch KOBIK)

Bei 89,1 Prozent aller Hausdurchsuchungen konnte illegales Material beschlagnahmt werden. Die Gründe für eine erfolglose Hausdurchsuchung sind vielfältig und nicht immer leicht zu eruieren. In den letzten Jahren verunmöglichten beispielsweise offene und ungeschützte Drahtlosnetzwerke eine eindeutige Identifizierung der Täterschaft. Für die Straftäter wird es dank kompakteren Speichermedien zunehmend leichter, belastendes Material effektiv zu verbergen. Zunehmend werden auch verschlüsselte Medien eingesetzt, welche die Beweiserbringung für den Besitz und den Austausch von verbotenen Erzeugnissen erschweren.

Bei den sichergestellten strafbaren Inhalten handelte es sich in 92,9 Prozent der Fälle, in denen verbotene Inhalte sichergestellt wurden, um pornografische Erzeugnisse mit Kindern. Da bei den aktiven Recherchen in P2P- und private P2P-Netzwerken gezielt nach Straftaten dieser Art gesucht wird und die Mehrheit aller Anzeigen aus diesen Recherchen stammen, erstaunt dieser hohe Prozentsatz nicht. Erwähnenswert ist jedoch, dass in mehr als 59,1 Prozent der Hausdurchsuchungen zusätzlich Vergehen gegen weitere Tatbestände der verbotenen Pornografie (Art. 197 StGB) festgestellt wurden.

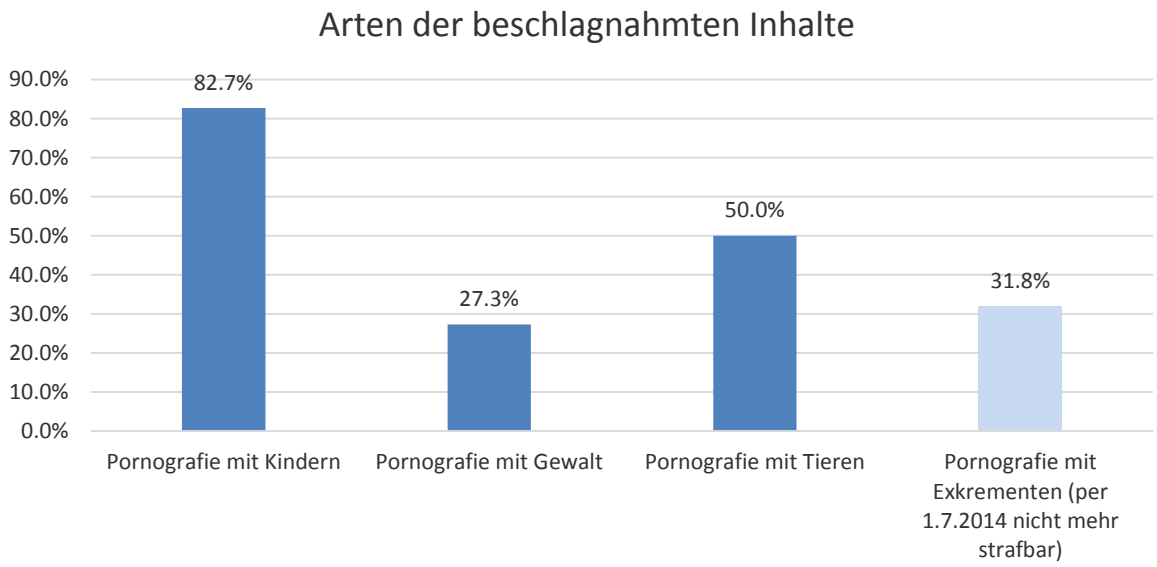


Abbildung 13: Prozentualer Anteil 2014 aller Hausdurchsuchungen, bei welchen verbotene pornografische Erzeugnisse sichergestellt wurden

Aus den Rückmeldungen der kantonalen Polizeibehörden geht weiter hervor, dass bei 57,1 Prozent der erfolgreichen Hausdurchsuchungen Videodateien, in 59,2 Prozent der Fälle Bilddateien und in 6,1 Prozent weiteres belastendes Material beschlagnahmt wurde. Insgesamt führten die Hausdurchsuchungen zur Sicherstellung von fast 700 000 strafbaren pornografischen Videos und Bildern.

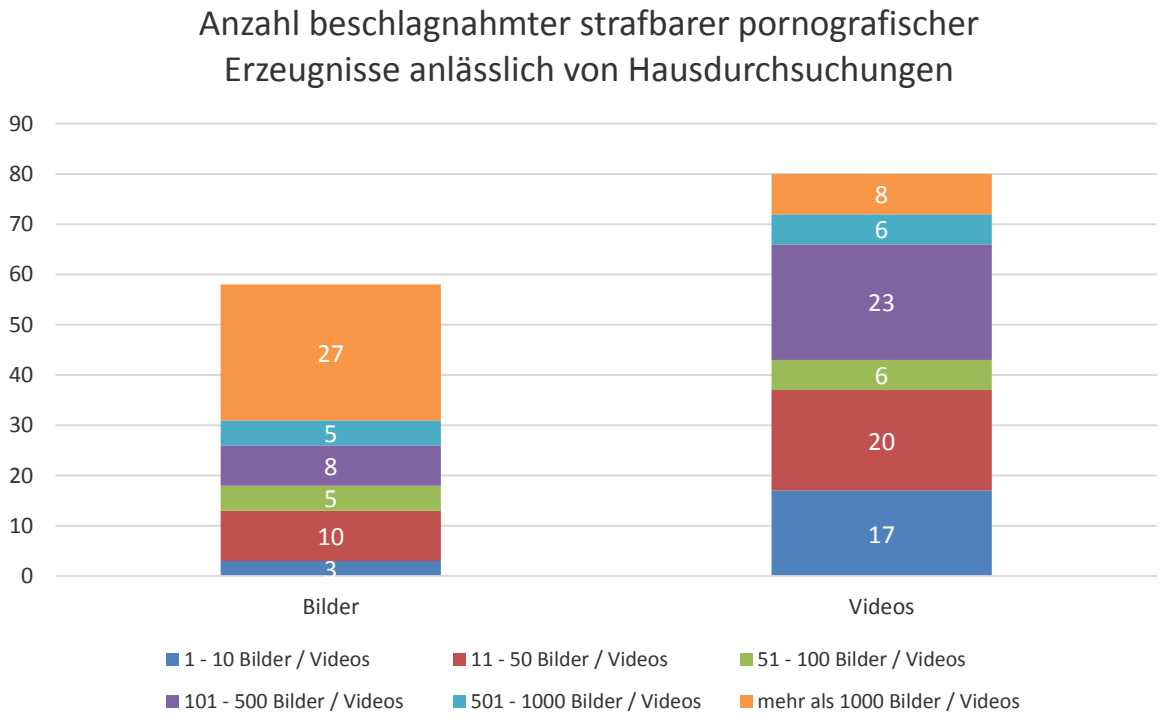
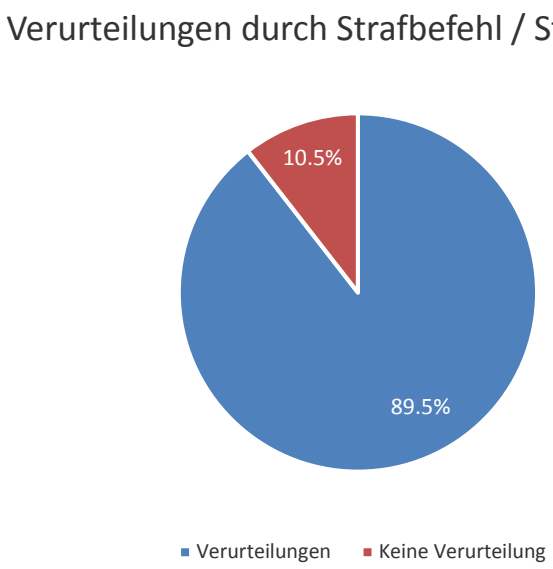


Abbildung 14: Aufschlüsselung der Mengen 2014 anlässlich von Hausdurchsuchungen beschlagnahmter pornografischer Erzeugnisse. Das Diagramm veranschaulicht, in wie vielen Fällen (gelistete Anzahl) inkriminierendes Material in welcher Menge (Farbe) vorgefunden wurde.

3.4.2 Rückmeldungen der kantonalen Justizbehörden

In 89,5 Prozent der Fälle, in denen die kantonalen Justizbehörden KOBIK eine Rückmeldung erstatteten, führten die Strafverfahren zu einer Verurteilung.



!

Abbildung 15: Verurteilungen 2014 durch ein Strafgericht oder einen Strafbefehl

Die meisten Verurteilungen wurden wegen Besitzes von harter Pornografie gestützt auf den Tatbestand der Pornografie (Art. 197 StGB) ausgesprochen und insbesondere aufgrund der in den Ziffern 3 und 3bis (vor der Revision des StGB) bzw. Abs. 4 und Abs. 5 (seit 1. Juli 2014) beschriebenen Tatbestände.

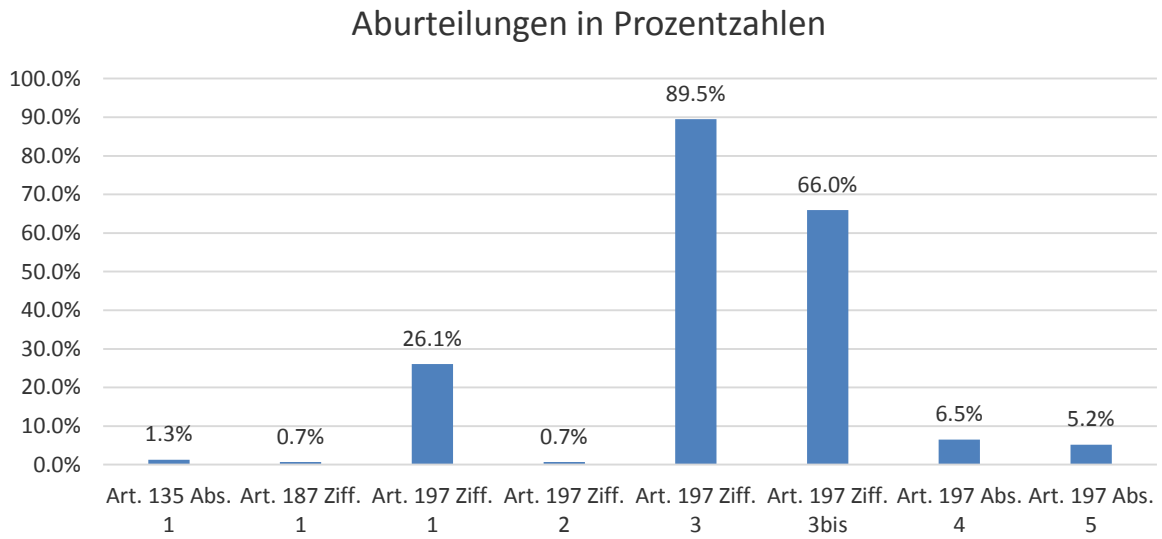
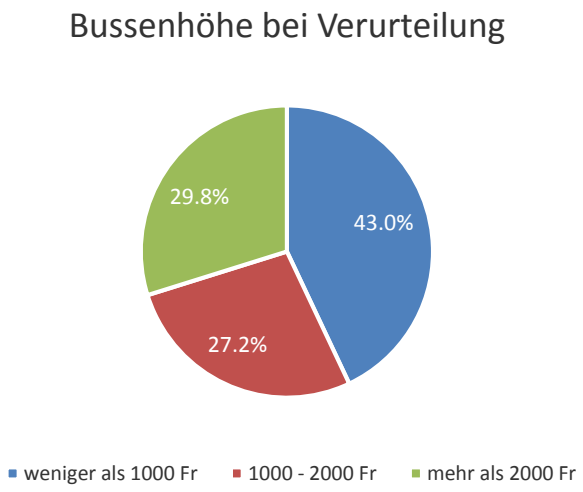


Abbildung 16: Häufigste Aburteilungen 2014 in Prozentzahlen. Die Grafik veranschaulicht, aufgrund welcher Artikel des StGB mit welcher Häufigkeit verglichen an der Gesamtzahl der Urteile ein Urteil gefällt wurde.

Bei 92,2 Prozent der 2014 gemeldeten Verurteilungen wurde eine Geldstrafe (Tagessatz) ausgesprochen. In 74,5 Prozent dieser Fälle wurde gleichzeitig eine Busse verhängt. Die Geldstrafen wurden bei 94,3 Prozent der Verurteilungen auf Bewährung ausgesetzt. Gemeinnützige Arbeit, Therapien, Freiheitsentzug (Gefängnis) oder nicht auf Bewährung ausgesetzte Geldstrafen wurden in 5,2 Prozent der Verurteilungen verhängt.



Abbildungen 17: Anzahl Tagessätze sowie Bussenhöhe bei Verurteilung im Jahr 2014

In etwa 43,0 Prozent der Fälle beliefen sich die Bussen auf weniger als 1000 Franken; in 27,2 Prozent auf 1000 bis 2000 Franken. Lediglich 29,8 Prozent der Bussen waren höher als 2000 Franken.

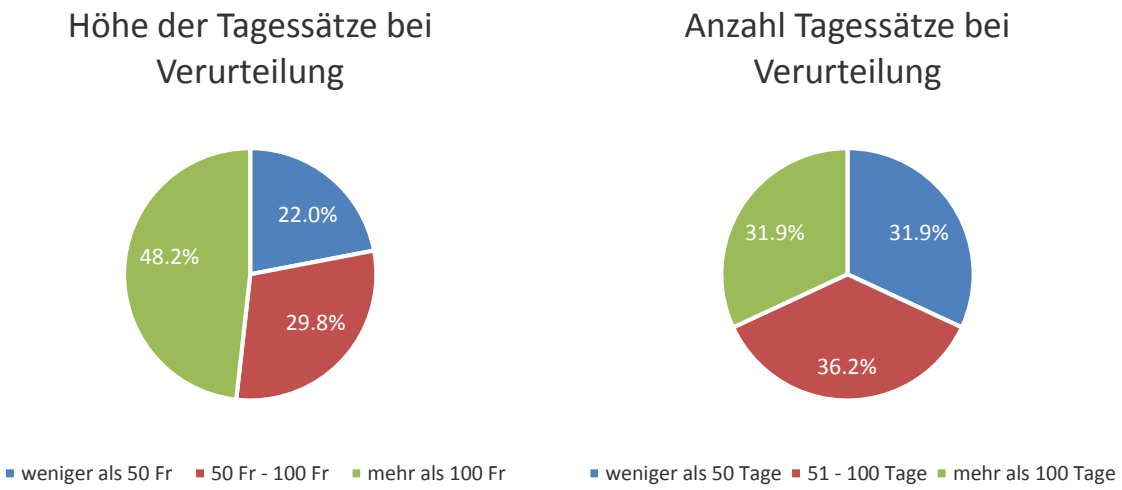


Abbildung 18: Verteilung der Höhe und Anzahl der bei einer Verurteilung festgelegten Tagessätze im Jahre 2014

31,9 Prozent der Geldstrafen wurden bei 50 oder weniger Tagessätzen festgelegt. Bei 36,2 Prozent wurden jeweils zwischen 51 und 100 Tagessätze angeordnet. Geldstrafen über mehr als 100 Tagessätze wurden in wiederum 31,9 Prozent der Fälle gesprochen.

In der Regel mussten die Verurteilten zusätzlich die Verfahrenskosten tragen, welche die eigentliche Busse oftmals um ein Vielfaches überstiegen.

3.5 Ausgewählte Fallbeispiele

Im Rahmen der durch KOBIK in privaten Tauschbörsen durchgeführten verdeckten Vorermittlungen gelang es, einen Benutzer in Österreich zu identifizieren. Dieser gewährte einem verdeckten Ermittler von KOBIK Zugriff auf seine umfangreiche Sammlung von Kinderpornografie. Die nachfolgend durchgeführten Ermittlungshandlungen ergaben einen Internetanschluss in Österreich, von welchem aus sich der Täter in die Tauschbörse eingewählt hatte. Die Übermittlung an die österreichischen Kollegen hatte zur Folge, dass durch das Landeskriminalamt Steiermark neben dem Verdächtigten gegen insgesamt 51 weitere Verdächtige in Schweden, den Niederlanden, Belgien, Dänemark, Brasilien und dem Iran ermittelt werden konnte.

In einem anderen Fall wurde im Rahmen einer Hausdurchsuchung nach einer Anzeige von KOBIK durch die zuständige Kantonspolizei kinderpornografisches Material sichergestellt. Da es sich beim Beschuldigten um den Ehemann einer Tagesmutter handelte, informierte die betroffene Gemeinde die Öffentlichkeit in einer Medienmitteilung über den Fall. Die Tagesfamilie hatte seit 2012 bereits drei Kinder in ihrer Obhut. Glücklicherweise ergaben sich durch die Ermittlungen der zuständigen kantonalen Behörden keine Hinweise auf Übergriffe auf weitere Kinder.

4 Kriminalpolizeilicher Informationsaustausch

4.1 Polizeilicher Meldungsein- und ausgang

Seit der Eingliederung in die Bundeskriminalpolizei im Jahr 2009 übernimmt KOBIK die Koordination des internationalen kriminalpolizeilichen Informationsaustauschs im Bereich der Internetkriminalität. In dieser Funktion unterstützt KOBIK als koordinierendes Kompetenzzentrum die Kantone in ihren Ermittlungen. Seit Inkrafttreten des Übereinkommens über die Internetkriminalität des Europarates (Budapest Convention on Cybercrime, Council of Europe, kurz: CCC) am 1. Januar 2012 wird die Schweiz international vermehrt als aktiver Partner in der Bekämpfung der Internetkriminalität wahrgenommen. Zur Erfüllung dieser Aufgaben verfügt KOBIK über ein grosses Netzwerk im In- und Ausland sowohl im öffentlichen Sektor, als auch in der Privatwirtschaft. Zudem bildet KOBIK die Schnittstelle für die Kantone zu den internationalen Organisationen INTERPOL und Europol in Sachen Cybercrime. Als einer der wichtigsten Partner hat sich dabei das European Cybercrime Center (EC3) von Europol etabliert.

Insgesamt sind 1314 Meldungen über die verschiedenen Kanäle eingegangen. Dies entspricht einem Anstieg von 77,8 Prozent gegenüber dem Vorjahr. Auch die Ausgänge sind um 35,8 Prozent auf 1285 Meldungen gestiegen. Diese Meldungen beinhalten den Informationsaustausch mit in- und ausländischen Behörden.

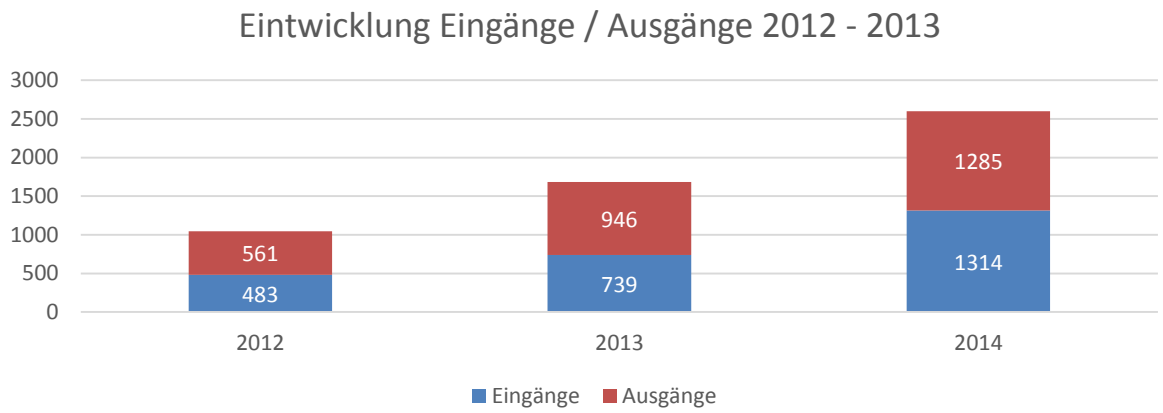


Abbildung 19: Entwicklung der Anzahl Meldungen im kriminalpolizeilichen Informationsaustausch 2012-2014

Eine Besonderheit der Budapest Convention on Cybercrime ist die Möglichkeit, auf polizeilichem Weg unter vorgängiger Ankündigung eines Rechtshilfeersuchens die sofortige Sicherstellung von Daten in den unterzeichnenden Staaten zu veranlassen (Art. 29 ff.). Diesbezüglich gingen bei KOBIK 15 Ersuchen aus den Kantonen an ausländische Behörden ein, die umgehend weitergeleitet wurden. Umgekehrt sind durch ausländische Behörden elf Ersuchen gestellt worden.

4.2 Nationale und internationale Verfahrenskoordination

Aufgrund der ein- und ausgehenden Meldungen im Rahmen des internationalen Informationsaustausches tätigt KOBIK laufend koordinierende Massnahmen. 2014 war dies in rund 146 Fällen der Fall. Die Art der gebotenen Unterstützung ist abhängig von der konkreten Ausgangslage. Insbesondere im Rahmen internationaler Ermittlungsverfahren nimmt KOBIK die

Rolle der zentralen Ansprechstelle für ausländische Polizeibehörden wahr und steht den nationalen Polizei- und Justizbehörden in der Schweiz in beratender Funktion zur Seite. In anderen Fällen, insbesondere solchen mit kantonaler Zuständigkeit, unterstützt KOBIK ersuchende Stellen mit analytischen, technischen und rechtlichen Expertisen oder dem Einsatz verdeckter Ermittler.

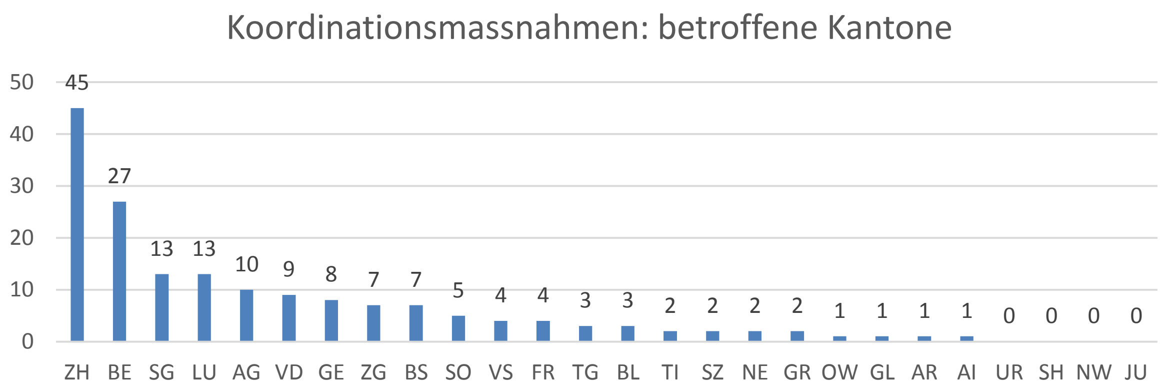


Abbildung 20: Von Koordinationsmassnahmen betroffene Kantone 2014. Da eine Koordinationsmassnahme mehrere Kantone betreffen kann, entspricht das Total der Grafik nicht dem oben aufgelisteten Total.

Ziel der von KOBIK getroffenen Massnahmen ist die Sicherstellung der optimalen Nutzung der bei den kantonalen Polizeistellen verfügbaren Ressourcen und das Verhindern von Doppelspurigkeiten in nationalen Ermittlungsverfahren. In diesem Rahmen organisierte KOBIK in zwei Fällen Koordinationssitzungen mit Vertretern der an den gleichen Fallkomplexen ermittelnden Kantonspolizeien.

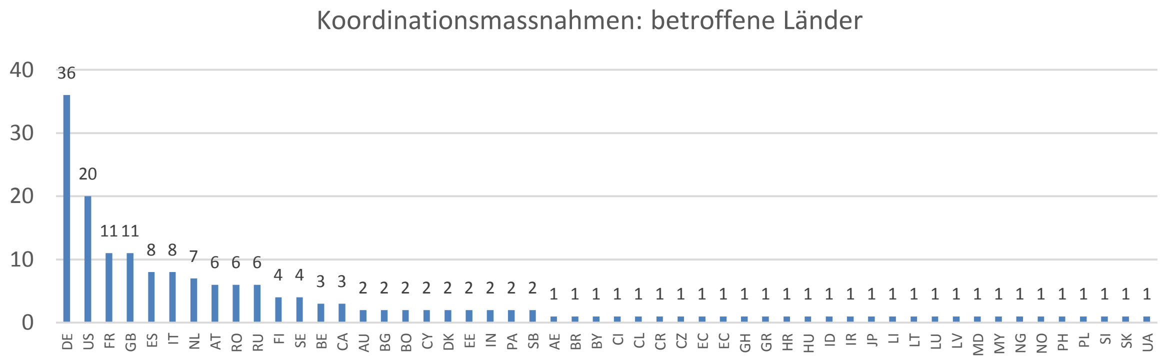


Abbildung 21: Von Koordinationsmassnahmen betroffene Länder 2014. Da mehrere Länder von einer Koordinationsmassnahme betroffen sein können, stimmt das Total der in der Grafik aufgelisteten Massnahmen nicht mit der oben genannten Zahl überein.

Die strafrechtliche Verfolgung einer aus dem Ausland agierenden und lose organisierten Täterschaft erfordert zahlreiche Ressourcen und grosses technisches Know-How. Die Verfolgung des Einzeldeliktes in einem Fallkomplex, beispielsweise ein einzelner Schadensfall in einer breit gestreuten Schadsoftware-Kampagne, ist aufgrund eines oftmals herrschenden Mangels an auswertbaren Spuren in der Regel zum Scheitern verurteilt. Erfahrungen in einem Fallkomplex zum Einsatz einer Schadsoftware gegen Kunden von Schweizer Banken zeigen die Bedeutung und den Aufwand des Führens einer nationalen Fallübersicht (vgl. Massnahme M6 der Strategie zum Schutz der Schweiz vor Cyberrisiken) auf. Eine zentrale Fallübersicht

ist sehr wichtig für die Erkennung von Zusammenhängen zwischen dem eigentlichen Schadsoftware-Angriff, der Verteilung der Schadsoftware via E-Mail oder präparierten Webseiten und der Auszahlung und des Transfers des gestohlenen Geldes. Erst die Analyse der durch eine systematische Sammlung von Anzeigen zum Gesamtphänomen gewonnenen Erkenntnisse führen die Ermittlungen zu weiterführenden Hinweisen. Da solche Fallkomplexe selten die Schweiz alleine betreffen sondern den gesamten deutsch- oder französischsprachigen europäischen Raum, ist eine internationale Zusammenarbeit und ein Informationsaustausch mit geeigneten Stellen, beispielsweise dem European Cybercrime Center EC3 bei Europol, unabdingbar und ressourcensparend.

4.3 Ausgewählte Fallbeispiele

Im Mai führte eine durch das US-amerikanische FBI koordinierte internationale Polizeiaktion in insgesamt 16 Ländern zur Verhaftung von rund 100 Anwendern der Schadsoftware «Blackshades». Im Vorfeld dieser Aktion stellte KOBIK anhand der vom US-amerikanischen FBI im Rahmen des internationalen kriminalpolizeilichen Informationsaustausches übermittelten Angaben Vorermittlungen über mögliche Schweizer Anwender der Schadsoftware an. Anhand dieser Vorermittlungen und nach einer von KOBIK einberufenen Koordinationssitzung mit zuständigen Staatsanwaltschaften und den betroffenen Polizeibehörden wurden in insgesamt 11 Kantonen Strafverfahren wegen Einfuhr von schädlicher Software gemäss Art. 144bis Ziff. 2 StGB gegen die mutmasslichen Käufer eröffnet. In einer zusätzlichen Koordinationssitzung wurden nach weiteren Ermittlungen erste Resultate durch die kantonalen Strafverfolgungsbehörden präsentiert sowie die Vorgehensweise für den eigentlichen Aktionstag abgesprochen. Am Aktionstag selber wurden durch die kantonalen Polizeibehörden gleichzeitig 16 Hausdurchsuchungen und anschliessende Befragungen durchgeführt. Die verhafteten Personen waren durchschnittlich 24-jährig, die Jüngste gar nur 16 Jahre alt. Aufgrund der bei den Hausdurchsuchungen sichergestellten Inhalte und den durchgeführten Befragungen liegen zudem bereits erste Urteile vor.

In einem anderen Fall erhielt KOBIK ein Ersuchen im Rahmen von Art. 29 und Art. 30 der Budapest Convention on Cybercrime. Im Zuge eines Ermittlungsverfahrens wurde durch die ersuchende ausländische Behörde festgestellt, dass in einem Fall von Erpressung ein Schweizer Internet-Dienst missbraucht worden ist, um ein erpresserisches Schreiben per E-Mail zu versenden. Das Ersuchen der ausländischen Behörde verlangte die Sicherung von Informationen, welche zur Identifizierung des Urhebers des erpresserischen Schreibens führen könnten. Der betroffene Dienst wurde von einer zunächst unbekannten Privatperson über eine Webseite betrieben, die bei einem Schweizer Provider gehostet wurde. Der Wohnsitz der Privatperson und der Standort der tatsächlichen Daten befand sich allerdings in zwei verschiedenen Kantonen, weshalb sich einerseits eine Koordination der Massnahmen auf polizeilicher, andererseits auf justizieller Ebene aufdrängte. In Zusammenarbeit mit den betroffenen Polizeistellen, den zuständigen kantonalen Staatsanwaltschaften und der Abteilung Internationale Rechtshilfe des Bundesamtes für Justiz gelang es, innert kürzester Zeit den privaten Betreiber des Dienstes zu identifizieren und mit einer Editionsverfügung für die Herausgabe der geforderten Daten zu bedienen. Mit Eintreffen einer digitalen Vorabkopie des in Aussicht gestellten Rechtshilfeersuchens der ersuchenden Behörde konnten schon am Folgetag die geforderten Daten auf polizeilichem Wege in Anwendung von Art. 30 der Budapest Convention on Cybercrime vorab übermittelt werden.

5 Projekte

5.1 NCS

Am 27. Juni 2012 hat der Bundesrat die Nationale Strategie zum Schutz der Schweiz vor Cyberrisiken (NCS) verabschiedet. Die Bekämpfung der Internetkriminalität ist dabei ein wichtiger Faktor zum Schutz der kritischen Infrastrukturen. Diesem Umstand wird durch die Massnahme 6 NCS Rechnung getragen. Zuständigkeitshalber wurde das EJPD mit der Umsetzung dieser Massnahme beauftragt. Hierfür soll ein Konzept in Zusammenarbeit mit den Kantonen erarbeitet werden, um eine aktuelle Fallübersicht zur Internetkriminalität in der Schweiz zu erlangen, damit interkantonale Fallkomplexe besser koordiniert werden können. Die gewonnenen Informationen aus der Strafverfolgung sollen in die gesamtheitliche Lagedarstellung bei MELANI einfliessen.

Dieses Konzept soll dem Bundesrat bis Ende 2016 vorgelegt werden. Es umfasst neben der beschriebenen Massnahme die Klärung von Schnittstellen mit weiteren Akteuren auf den Gebieten der Minimierung von Cyberrisiken, der Koordination mit der Lagedarstellung und der für die Umsetzung des Konzepts benötigten Ressourcen und rechtlichen Anpassungen auf Stufe Bund und Kantone.

Die Arbeiten zur Erstellung des Konzeptes zu Massnahme 6 NCS konnten erfolgreich initiiert werden. Anfang Mai 2014 hat KOBIK eine nationale Umfrage bei sämtlichen Strafverfolgungsbehörden von Bund und Kantonen lanciert. Der so erkannte Ist-Zustand und die Schwachstellen und Bedürfnisse der an der Bekämpfung der Internetkriminalität beteiligten Stellen sind ins Konzept eingeflossen.

Da sich die Projektarbeiten aufgrund der Komplexität des Auftrages umfangreicher als erwartet gestalten, musste die Vernehmlassung bei den Kantonen auf das erste Quartal 2015 verschoben werden.

Die Schlussrevision des Konzepts soll ab September 2015 vorliegen. Anschliessend wird das Projekt dem Bundesrat vorgelegt.

6 Arbeitsgruppen, Partnerschaften und Kontakte

6.1 Nationale Datei- und Hashwertesammlung (NDHS)

KOBIK betreibt in Zusammenarbeit mit den Kantonen eine Sammlung von Hashwerten (auch Hash-Codes genannt) von eindeutig als verbotene Pornografie kategorisierten Bildern. Ziel dieser Sammlung ist es, die psychische Belastung und den Arbeitsaufwand für die in Fällen von Verbreitung von Kinderpornografie eingesetzten Ermittlern zu reduzieren. Dazu werden Bilder, deren Hashwert bereits in der NDHS registriert ist, automatisch kategorisiert. Die NDHS befindet sich seit Oktober 2012 im produktiven Betrieb und steht den kantonalen und städtischen Fachstellen der Polizeikorps zur Verfügung.

Mit Inkrafttreten der Änderungen von Art. 197 des Strafgesetzbuches vom 1. Juli 2014 wurde das Verbot der Pornografie mit Ausscheidungen aufgehoben. Entsprechend musste die NDHS angepasst und die zuvor darin erfassten Hashwerte von Bildern dieser Kategorie gelöscht werden.

Den Kantonen werden nur diejenigen Hashwerte zur Verfügung gestellt, deren zugehörige Bilder schon dreimal als eindeutig verboten bewertet wurden. Die Kategorisierung nimmt einige Zeit in Anspruch. Zudem bedingt der anvisierte internationale Austausch neben einer einheitlichen Kategorisierung auch einen verlässlichen Qualitätsstandard. Ziel dieser Massnahmen ist es auch, dass Hashwerte eindeutig verbotener Erzeugnisse in Gerichtsakten einfliessen können.

Bis Ende 2014 wurden insgesamt rund vier Millionen Dateien angeliefert und deren Hashwerte in die NDHS eingegeben. Die Kategorisierung des Bildmaterials erweist sich als zeitaufwändig und kann nur dank der solidarischen Unterstützung der Kantone sichergestellt werden. Damit ein Bild eindeutig als verbotene Pornografie eingestuft wird, bedarf es dreier gleicher Wertungen durch Mitarbeitende der kantonalen Polizeistellen oder KOBIK. Bis heute wurden etwa 138 000 Bilder dreimalig bewertet und damit als eindeutig verbotene Pornografie in der NDHS erfasst.

Des Weiteren stellt KOBIK den Kantonen zirka drei Millionen ausländische Hashwerte zur forensischen Untersuchung zur Verfügung. Diese wurden durch ausländische Strafverfolgungsbehörden errechnet und an KOBIK ausgeliefert. Da jedoch das zugehörige Bildmaterial nicht vorhanden ist, können bei diesen Hashwerten keine Qualitätskontrollen durchgeführt werden. Deshalb handelt es sich hierbei im Gegensatz zu den bestätigten Hashwerten der NDHS um sogenannte Verdachtshashwerte. Zusätzlich stellt KOBIK 78 Millionen so genannte Whitelist-Hashwerte zur Verfügung. Bei den Whitelist-Hashwerten handelt es sich um Kennwerte, die nicht strafbare Inhalte (z.B. Icons von Betriebssystemen oder Applikationen) bezeichnen. Diese White-Listen dienen zur automatischen Reduktion der durch die Forensiker aufzubereitenden Dateien. KOBIK beschafft sich systematisch solche White-Listen und stellt sie den Kantonen zeitgleich mit den Black-Listen zur Verfügung.

Zurzeit erarbeitet KOBIK in Zusammenarbeit mit den Kantonen ein Konzept zur Erweiterung dieser Datensammlung im Hinblick auf eine systematische Opferidentifikation und einen Abgleich mit der INTERPOL-Datenbank ICSE[9]. Diese Arbeiten stehen im Zusammenhang mit den Zielsetzungen der Global Alliance (Siehe Punkt 6.7.3), deren Umsetzung für die Schweiz unter anderem vorsieht, ein nationales Opferidentifikationskonzept in Zusammenarbeit mit den Kantonen bis im Jahr 2016 zu erarbeiten.

[9] ICSE - International Child Sexual Exploitation image database

Neben den Hashwerten und deren Bedeutung für die forensische Durchforstung von sichergestelltem Material bietet eine zentrale Bilddatenbank viele Ermittlungsansätze zur Identifikation der Täter und deren Opfer, die aufgrund des anfänglich unbekannten Tatortes nicht immer im geographischen Zuständigkeitsbereich der ursprünglich ermittelnden Behörde missbraucht wurden. Es ist international anerkannt, dass auf Opferidentifikation ausgerichtete Ermittlungen anhand von sichergestelltem Bildmaterial und länderübergreifender Zusammenarbeit sehr erfolgsversprechend sind. Zudem erscheint es auch aus ethisch-moralischer Sicht gerechtfertigt, vorhandene Ressourcen für die Identifikation von Kindern einzusetzen, die zum Zeitpunkt der Sicherstellung oder der Sichtung des Bildmaterials womöglich immer noch sexuell missbraucht werden; dies auch wenn sich herausstellt, dass der Missbrauch nicht im eigenen Zuständigkeitsbereich stattgefunden hat. So können Opfer darauf zählen, dass die Strafverfolgungsbehörden unabhängig einer ihnen bekannten geographischen Zuständigkeit, ihre Arbeit aufnehmen, um weiteren Missbräuchen vorzubeugen und Täter zu verhaften. Es gilt, die gemeinsame Verantwortung für ein globales Phänomen wahrzunehmen und den eigenen Handlungsspielraum möglichst auszuschöpfen.

Bei der Opferidentifikation in der Schweiz besteht noch Entwicklungspotential. Mit der NDHS wurde der erste Grundstein für eine systematische Opferidentifikation gelegt. Die zahlreichen Online-Angebote wie Foren, Peer-to-Peer Austauschbörsen, soziale Medien und anonyme Netzwerke zur zwischenmenschlichen Interaktion werden aber leider nach wie vor zu oft durch Menschen missbraucht, die Kindern schaden wollen.

Mit der NDHS hat die Schweiz einen wichtigen Grundstein zur Bekämpfung der Herstellung, des Handels und der Verbreitung von illegalem Bildmaterial bzw. des Kindsmissbrauchs im Internet und der immer wiederkehrenden «Reviktimisierung» der Kinder gelegt. Mit ihrer Teilnahme an der Konferenz des Globalen Bündnisses gegen den Kindsmissbrauch online vom 6. Dezember 2012 hat Bundesrätin Simonetta Sommaruga den Willen der Schweiz bekräftigt, diesen Kampf auf nationaler und internationaler Ebene zu unterstützen.

6.2 Nationale Arbeitsgruppen

KOBIK war im Berichtsjahr in verschiedenen nationalen Arbeitsgruppen vertreten.

Gemeinsam mit dem Kommissariat Pädokriminalität/Pornografie der Bundeskriminalpolizei ist KOBIK Mitglied und Organisator der Arbeitsgruppe «Kindsmissbrauch». In der Arbeitsgruppe sind Strafverfolgungsbehörden des Bundes und der Kantone, die Schweizerische Kriminalprävention und gemeinnützige Organisationen aus dem Bereich Kinderschutz vertreten.

Wie bereits in den Vorjahren war KOBIK auch 2014 im nationalen Programm «Jugendmedienschutz und Medienkompetenzen» sowohl in der mit der Programmausarbeitung vertrauten Steuergruppe, als auch in der ausführenden Projektgruppe «Monitoring der Regulierung und Medienentwicklung» vertreten. Das Programm soll Kindern und Jugendlichen helfen, einen sicheren, verantwortungsvollen und dem Alter angepassten Umgang mit den neuen Medien zu finden.

6.3 Bundesinterne Zusammenarbeit

Die Internetkriminalität betrifft fast sämtliche Titel des Strafgesetzbuches. Entsprechend vielfältig ist die Zusammenarbeit, die KOBIK innerhalb der Bundesverwaltung betreibt. Innerhalb von fedpol steht vor allem die intensive Zusammenarbeit mit den Kommissariaten Pädokriminalität/Pornografie, IT-Ermittlungen und Verdeckte Ermittlungen der Bundeskriminalpolizei im

Vordergrund. Zudem ist KOBIK mit der fedpol-Hauptabteilung Internationale Polizeikooperation (IPK) in engem Kontakt. Wie auch im letzten Jahr wurden die Kontakte mit diversen Bundesstellen intensiviert. Diese beinhalten unter anderem MELANI, die Abteilung Internationale Rechtshilfe im Bundesamt für Justiz (BJ), die Finanzmarktaufsicht (FINMA), das Institut für geistiges Eigentum (IGE) und die Eidgenössische Spielbankenkommission (ESBK), das Eidgenössische Departement für auswärtige Angelegenheiten (EDA) und den Sicherheitsverbund Schweiz (SVS).

6.4 Erfahrungsaustausch mit den Kantonen

Im Berichtsjahr pflegte KOBIK zahlreiche Kontakte mit Vertretern diverser Polizeikorps und Staatsanwaltschaften. Ein Grossteil dieser Kontakte wurde im Zusammenhang mit laufenden operativen Fällen geknüpft. Hierbei konnten einerseits die Kantone vom Fachwissen und dem internationalen Kontaktnetz der KOBIK-Mitarbeitenden profitieren. Umgekehrt konnte KOBIK einen grossen Nutzen aus der Kenntnis der lokalen Gegebenheiten, der eingespielten Prozesse zwischen Polizei und Staatsanwaltschaft und auch dem in den Kantonen vorhandenen forensischen Know-How ziehen.

Dank der koordinierenden Funktion von KOBIK und der guten Zusammenarbeit mit den Kantonen gelang es, in mehreren Fällen (siehe auch Abschnitt 5.3) eine Beweisvernichtung durch Verdächtige zu verhindern oder die Eröffnung eines Strafverfahrens aufgrund eines aus dem Ausland gemeldeten Sachverhaltes zu ermöglichen.

6.5 Zusammenarbeit mit NGOs und Vereinen

Seit mehreren Jahren arbeitet KOBIK bei der Bekämpfung der Verbreitung von Kinderpornografie eng mit der NGO[10] Action Innocence Genève (AI) zusammen. Dank der Unterstützung durch AI konnte das Projekt zum Monitoring von Peer-to-Peer-Netzwerken in den letzten Jahren erfolgreich betrieben und weiterentwickelt werden.

Mit dem Verein «Stop Piracy» pflegt KOBIK einen engen Kontakt, um betrügerische Onlineshops, welche gefälschte Markenprodukte zum Kauf anpreisen, den zuständigen Polizeibehörden oder Hosting-Providern zu melden.

Ebenso strebt KOBIK eine Zusammenarbeit mit dem Verein «Swiss Internet Security Alliance» (SISA) an. Dieser stellt einen Verbund von ISPs, Internetdienstleistern und Informationssicherheits-Experten dar, der zum Ziel hat, das Schweizerische Internet zu einem Schadsoftware-freien Raum werden zu lassen.

6.6 Zusammenarbeit mit den Schweizerischen Internet-Zugangs-Anbietern (ISPs)

Seit 2007 besteht zwischen KOBIK und den grössten Schweizer Internetanbietern ein Abkommen über die Blockade von Internetseiten mit verbotenen kinderpornografischen Inhalten. Die Sperre richtet sich dabei ausschliesslich gegen ausländische Internetseiten, die verbotene Pornografie mit Kindern gemäss Art. 197 Abs. 4 und 5 zum Download anbieten. Die Internetanbieter blockieren aufgrund ihrer allgemeinen Geschäftsbedingungen und ethischen Grundsätzen den Zugang zu strafrelevanten Seiten und leiten den Benutzer auf eine «Stopp-

[10] Non-Governmental Organization (Nichtregierungsorganisation)

Seite» weiter. KOBIK erstellt und unterhält diesbezüglich eine laufend aktualisierte Liste, die zwischen 700 bis 1000 Webseiten enthält.

Im Rahmen dieses Projekts arbeitet KOBIK eng mit INTERPOL zusammen. Die in der Schweiz erstellte Liste alimentiert zu einem grossen Teil die INTERPOL-«Worst-Of»-Liste von Webseiten, die kinderpornografische Inhalte anbieten. KOBIK sucht täglich proaktiv neue Internetseiten mit kinderpornografischen Inhalten und ergänzt laufend die INTERPOL-Liste, die in Zusammenarbeit mit mehreren Ländern unterhalten wird.

6.7 Internationale Zusammenarbeit

6.7.1 Europol

Seit 2011 ist KOBIK Mitglied in verschiedenen Arbeitsgruppen rund um das European Cybercrime Center (EC3). Dieses bei Europol in den Haag angesiedelte Zentrum zur Bekämpfung der Internetkriminalität unterstützt EU- und Drittstaaten operationell und stellt Fachwissen und Analysetätigkeiten für gemeinsame Untersuchungen auf EU-Ebene zur Verfügung. KOBIK pflegt einen intensiven Kontakt mit dem EC3 und hat im Berichtsjahr regelmässig an strategischen und operationellen Treffen teilgenommen. Die vom EC3 festgesetzten Schwerpunkte liegen dabei grundsätzlich in der Bekämpfung von Phänomenen der «Internetkriminalität im engeren Sinne» durch den Focal Point CYBORG, des «systematischen Missbrauchs von Kreditkarten» durch den Focal Point TERMINAL und der «gewerbsmässigen und organisierten Verbreitung von Kinderpornografie» durch den Focal Point TWINS.

KOBIK ist Mitglied des Focal Point (FP) «CYBORG» des EC3, dessen Ziel die Bekämpfung von grenzüberschreitender Internetkriminalität im engeren Sinne ist. Dabei liegt der Fokus auf den Phänomenen «Phishing», «DDoS», «Botnetze», «Hacking» und weiteren.Zusätzlich ist KOBIK zusammen mit dem Kommissariat PP der Bundeskriminalpolizei Mitglied des FP «TWINS», der sich der Bekämpfung der Pädokriminalität im Internet widmet.

6.7.2 Beitritt der Schweiz zur Virtual Global Taskforce (VGT)

Die rasante Entwicklung des Internets bietet der Täterschaft immer wieder neue Möglichkeiten, den Strafverfolgungsbehörden eine Nasenlänge voraus zu sein und sich an Kindern zu vergehen. Die VGT ist ein Zusammenschluss von Strafverfolgungsbehörden, NGOs und der Privatwirtschaft zur Bekämpfung des (sexuellen) Missbrauchs von Kindern im Internet und damit eine direkte Antwort auf diese Entwicklung.

Durch diese internationale Partnerschaft von Strafverfolgungsbehörden, NGOs und der Industrie zum Schutz der Kinder vor Online-Missbrauch macht die VGT das Internet sicherer. Missbräuche können schneller erkannt und lokalisiert, Kindern in Not geholfen und eine effiziente Strafverfolgung der Täterschaft gefördert werden.

Die Schweiz ist seit 2012 Mitglied der Global Alliance zum Schutz gegen den Online-Kindsmissbrauch und nimmt so ihren Teil dieser gemeinsamen Verantwortung im Kampf gegen den Kindsmissbrauch über das Internet wahr. Eines der anvisierten Ziele der Schweiz war die Mitgliedschaft in der VGT, die 2014 realisiert werden konnte.

Abbildung 22: Am 13. Mai 2014 unterzeichnet Thomas Walther, Kommissariatsleiter KOBIK, in Brüssel die Beitrittserklärung der Schweiz zur Virtual Global Taskforce in der Gegenwart von Anthony L. Gardner (links im Bild), US Botschafter für die Europäische Union, Roberto Balzaretti, Schweizer Botschafter für die Europäische Union (rechts) und Ian Quinn, Vorsitzender der VGT (zweiter von links).

Zu den Mitgliedern der VGT gehören neben der Schweiz auch Australien, Grossbritannien, Italien, Kanada, Kolumbien, Korea, die Niederlande, Neuseeland, die Vereinigten Arabischen Emirate, die Vereinigten Staaten von Amerika und Europol und INTERPOL.

Mitglieder aus dem Privatsektor sind End Child Prostitution, Child Pornography and Trafficking of Children for Sexual Purposes network (ECPAT International), International Association of Internet Hotlines (INHOPE), National Center for Missing & Exploited Children (NCMEC), International Centre for Missing and Exploited Children (ICMEC), PayPal, Microsoft Digital Crimes Unit, World Vision, Blackberry, The Code, Kids Internet Safety Alliance (KINSA), NetClean, International Justice Mission und Telstra.

Weitere Informationen zur VGT finden sich unter www.virtualglobaltaskforce.com.

6.7.3 Global Alliance against Child Sexual Abuse Online

Auf Einladung von EU-Kommissärin Cecilia Malmström und US-Justizminister Eric Holder Jr. trafen sich am 30. September 2014 Vertreter und Experten aus über 40 Ländern zur zweiten Ministerkonferenz der «Global Alliance against Child Abuse Online» in Washington DC, USA.

Anlässlich der Ministerkonferenz gaben Referenten aus der Strafverfolgung, der Privatwirtschaft und Nicht-Regierungsorganisationen Einblicke in die erzielten Erfolge aus den vier Fokusbereichen der Allianz (Opferidentifikation, Täteridentifikation und -verfolgung, Sensibilisierung, Vermeidung der Reviktimisierung). In seiner Eröffnungsrede zeigte sich US General Attorney Eric Holder Jr. stolz über die erzielten Erfolge und Entwicklungen seit der Initialisierung der Global Alliance. Seit 2012 haben sich bereits 54 Länder der Allianz angeschlossen und

gehen nun gemeinsam und aktiv gegen die globale Problematik des Online-Kindsmissbrauchs vor. Holder betonte, dass man sich trotzdem nicht zufrieden geben dürfe, denn die Gefahren des Missbrauchs von Kindern hätten sogar noch zugenommen. Hervorzuheben sei hier insbesondere die Problematik der Kinderpornografie im Internet, die sich ungehindert weiterverbreitet und dadurch zu einer dauernden Viktimisierung der Kinder führt. Die Allianz alleine werde die Problematik der Kinderpornografie im Internet jedoch nicht lösen können und sehe sich deshalb als Ergänzung zu bereits bestehenden internationalen Strukturen und Abkommen.

Das globale Bündnis legt politische sowie operative Ziele fest, stellt es den einzelnen Ländern aber frei, wie sie diese umzusetzen und zu erreichen gedenken. Die von der Schweiz gesteckten Ziele konnten 2014 in sämtlichen Bereichen erreicht oder sogar übertroffen werden. Dies hat international zu einer hohen Anerkennung unseres Landes im Bereich der Bekämpfung dieses Bereichs der Cyberkriminalität geführt. So wurde die Schweiz anlässlich diverser Präsentationen namentlich erwähnt und hervorgehoben und hat sich bei der Bekämpfung des Online-Kindsmissbrauchs in den letzten zwei Jahren zur internationalen Spitze gesellt.

Auf Initiative des Britischen Premierministers David Cameron und in Analogie zu den Zielen der Global Alliance, fand am 10. und 11. Dezember 2014 der #WePROTECT Children Online Global Summit in London statt. Im Gegensatz zur Global Alliance liegt der Fokus bei #WePROTECT nicht auf den Strafverfolgungsbehörden, sondern auf den Teilnehmern aus der Privatwirtschaft. Die führenden Technologieunternehmen haben dabei nicht nur ihre Bereitschaft zur Unterstützung in dieser Sache proklamiert, sondern auch zusammen mit den anwesenden Vertretern der Strafverfolgungsbehörden sowie privaten Organisationen ein «Statement of Action» unterzeichnet[11].

6.7.4 US FBI & Homeland Security

Aufgrund der Tatsache, dass die meisten der grossen Internet-Dienstleistungsanbieter in den USA ansässig sind und die USA ebenfalls eine intensive Zusammenarbeit mit Europol und den Mitgliederstaaten im Bereich Cybercrime anstreben, steht KOBIK mit dem Büro des FBI Legal Attaché in Bern in regem Kontakt. Nebst dem kriminalpolizeilichen Informationsaustausch pflegt KOBIK einen informellen Austausch rund um Best-Practice für Datensicherungen bei den grossen amerikanischen Dienstleistern. Umgekehrt werden Anfragen aus der USA zur Sicherung von Daten bei Schweizer Internetanbietern direkt über den Legal Attaché an die Einsatzzentrale fedpol weitergeleitet und von KOBIK bearbeitet.

Des Weiteren steht KOBIK in engem Kontakt mit dem in Rom stationierten Attaché des US Immigration and Customs Enforcement unter dem Departement Homeland Security, der die Verbindung zu der zugehörigen Cybercrime Abteilung sicherstellt. Deren Direktor übt zur Zeit die Präsidentschaft der VGT aus.

[11] Statement of Actions in Englischer Sprache einsehbar unter https://www.gov.uk/government/publications/weprotect-summit

7 Medienauftritte, Ausbildung und Konferenzen

7.1 Medienpräsenz

Im Berichtsjahr wurde in zahlreichen Medienberichten über die Tätigkeiten von KOBIK berichtet. Insgesamt wurden durch Mitarbeitende von KOBIK rund hundert Medienanfragen beantwortet.

Erwähnenswert sind insbesondere auch die von KOBIK erstellten Warnmeldungen zu kriminellen Phänomenen im Internet, die teilweise auch den Medien und weiteren Partnerorganisationen wie MELANI und der Schweizerischen Kriminalprävention SKP zur Kenntnis gebracht wurden. Warnmeldungen werden hauptsächlich erstellt, wenn KOBIK eine Häufung eingehender Meldungen zu einem bestimmten Phänomen feststellt. Ein weiterer Anlass sind bestimmte Zeitperioden, beispielsweise bevorstehende Festtage, die bekannt dafür sind, dass bestimmte Deliktsformen gehäuft auftreten. Im Berichtsjahr warnte KOBIK beispielsweise vor E-Mails mit Schadsoftware, die mit angeblich unbezahlten Rechnungen von Versandhäusern, Telekom-Anbietern und weiteren versandt wurden sowie vor Häufungen von Betrugsversuchen und gefälschten Online-Shops in der Vorweihnachtszeit.

Um die grössten Schweizer Verlagshäuser sind mehrere Digital-Ressorts entstanden, welche sich Cyber-Themen annehmen und diese einem weiten Teil der Bevölkerung zugänglich machen. Zudem wurden in den letzten Jahren mehrere Personen von öffentlichem Interesse Opfer von Cyberkriminellen. Die Social-Media-Auftritte von KOBIK, insbesondere Twitter, werden von Online-Redaktionen in der Schweiz und im Ausland aktiv besucht. Von KOBIK publizierte Warnmeldungen werden auf den Medien-eigenen Kanälen weiter verbreitet und enthalten oft auch den Hinweis auf das Meldeformular.

7.2 Social Media

Seit 2013 ist KOBIK auf den Social-Media-Plattformen Facebook (www.facebook.com/cybercrime.ch) sowie auf Twitter (@KOBIK_Schweiz) aktiv. Die Plattformen werden insbesondere zur schnellen Verbreitung von Hinweismeldungen über aktuelle Phänomene genutzt, um die Schweizer Bevölkerung vor häufig gemeldeten Betrugsmaschen oder aktuellen Schadsoftware-Kampagnen zu warnen. Das bisherige Echo ist durchwegs positiv.

Nach etwas über einem Jahr Laufzeit zählten die deutsch-, italienisch- und französischsprachigen Auftritte auf Facebook insgesamt bereits 3576 Likes und das mehrsprachige Twitter-Profil 487 Follower.

7.3 Ausbildungen und Konferenzen

KOBIK-Mitarbeitende nahmen an mehreren internationalen Konferenzen und Tagungen sowie Ausbildungslehrgängen teil. Sie nutzten diese Gelegenheiten insbesondere zur persönlichen Weiterbildung, aber auch zur Kontaktpflege und Informationsaustauschaber mit Partnern und Experten im Bereich Cybercrime, Kinderschutz und Opferidentifikation.

Mitarbeitende von KOBIK waren weiter an diversen Anlässen als Ausbildner aktiv. Beispielsweise führten zwei Mitarbeiter einen zweitägigen von der Schweiz organisierten Kurs für die Mitteleuropäische Polizeiakademie (MEPA) in Sachen Open Source Intelligence im Internet

durch. In über hundert weiteren Anlässen nahmen Mitarbeiter von KOBIK als Experten, Ausbildner oder Fachreferenten teil.

Weiter fand am 13. November 2014 zum dritten Mal das durch KOBIK organisierte «Forum Cybercrime Staatsanwaltschaften – KOBIK» statt. Internationale Experten aus der Strafverfolgung präsentierten den Teilnehmenden einen praxisnahen Einblick in die internationale Bekämpfung der Internetkriminalität. Zudem wurde das mobile Labor zur Identifizierung von Opfern auf kinderpornografischen Aufnahmen von INTERPOL präsentiert und praktische Übungen angeboten. In der anschliessenden Podiumsdiskussion wurde die Revision des BÜPF (Bundesgesetz zur Überwachung des Post- und Fernmeldeverkehrs) diskutiert. Am Forum haben rund hundert Personen teilgenommen.

Am darauffolgenden Tag, 14. November 2014, wurde ebenfalls unter Mitwirkung von INTERPOL ein Opferidentifikationstag für Angehörige der kantonalen und städtischen Polizeikorps durch KOBIK in Bern durchgeführt. Der Opferidentifikationstag ist ein direktes Resultat des Beitritts der Schweiz zur «Global Alliance against Child Sexual Abuse Online» (vgl. 6.7.3 Global Alliance) und den damit in Verbindung stehenden Massnahmen und Verpflichtungen. Diese sehen unter anderem verstärkte Bemühungen vor, Opfer von Kinderpornografie zu identifizieren und deren Erhalt von Schutz, Betreuung und Unterstützung zu gewährleisten. Ziel des Opferidentifikationstages war es, auf eine proaktive und systematische Identifikation von Opfern von Kinderpornografie im Internet nach internationalem Muster hinzuarbeiten. Dazu sollte festgestellt werden, ob Synergien zwischen Bildkategorisierung in der NDHS und Opferidentifikation in Zusammenarbeit mit der von INTERPOL zur Verfügung gestellten ICSE-Datenbank genutzt werden können. Zu einem späteren Zeitpunkt soll ein Kooperations- und Opferidentifikationskonzept im Hinblick auf ein arbeitsteiliges Vorgehen bis Ende 2016 gemeinsam mit den Kantonen erarbeitet werden.

Im Zusammenhang mit der NDHS veranstaltete KOBIK über das ganze Jahr Ausbildungen in der Kategorisierung von Bild- und Videomaterial für Ermittler verschiedenster Schweizer Polizeikorps und Vertreter von Privatfirmen, welche die forensische Auswertung von sichergestelltem Material sowie die damit verbundene Kategorisierung von Bildmaterial im Auftrag kantonaler Staatsanwaltschaften übernehmen. Dies mit dem Ziel, dass die Kategorisierung von verbotener Pornografie in der NDHS schweizweit nach den gleichen Kriterien erfolgt und somit die qualitative Zuverlässigkeit der NDHS sichergestellt werden kann. Während des zwei Halbtage dauernden Kurses werden die Kursteilnehmer unter anderem in rechtlichen Belangen geschult und haben ausgiebig Gelegenheit, selber Bildmaterial zu kategorisieren und strittige Fälle mit den Ausbildern zu diskutieren.

8 Politische Vorstösse auf Bundesebene

8.1 Auflistung relevanter parlamentarischer Vorstösse

Motion 14.3022: Kinderpornografie. Verbot von Posing-Bildern – Rickli Natalie Simone, 3.3.2014

Frage 14.5175: Cyberrisiken. Plattform Tumblr – Schmid-Federer Barbara, 12.3.14

Interpellation 14.3204: Konsens der Arbeitsgruppe Agur 12. Weiteres Vorgehen – Gutzwiller Felix, 20.3.14

Postulat 14.3193: Verbesserung der polizeilichen Ermittlungen in sozialen Netzwerken – Vogler Karl, 20.3.14

Interpellation 14.3250: Jugendgewalt. Was tun? – Grin Jean-Pierre, 21.3.14

Motion 14.3288: Identitätsmissbrauch. Eine strafbare Handlung für sich – Comte Raphaël, 21.3.14

Motion 14.3367: Sexting bekämpfen – Amherd Viola, 8.5.14

Postulat 14.3655: Die digitale Identität definieren und Lösungen für ihren Schutz finden – Derder Fathi, 20.6.14

Motion 14.3665: Ergänzung von Artikel 260bis StGB (Art. 187 StGB, “Sexuelle Handlungen mit Kindern“) – Kommission für Rechtsfragen NR, 14.8.14

Motion 14.3666: Artikel 198 StGB. Von Antrags- zu Offizialdelikt – Kommission für Rechtsfragen NR, 14.8.14

Interpellation 14.3888: Internationale Bekämpfung von Hasspropaganda im Internet – Naef Martin, 25.9.14

Motion 14.3905: Identifizierung der Verfasser von Hassnachrichten im Internet gewährleisten – Schwaab Jean Christophe, 25.9.14

Postulat 14.3908: Internet. Intoleranz nicht tolerieren – Tornare Manuel, 25.9.14

Postulat 14.3962: Internationale Amtshilfe bei Straftaten gegen Kinder im Internet verbessern – Müller-Altermatt Stefan, 26.9.14

Postulat 14.3963: Wie verstecken sich Pädophile hinter dem Datenschutz – Müller-Altermatt Stefan, 26.9.14

Interpellation 14.3969: Mit Medienkompetenz gegen Hasskampagnen – Masshardt Nadine, 26.9.14

9 Denkbare Entwicklungen

Die Zahl der KOBIK erstatteten Meldungen hängt nicht zuletzt davon ab, wie geneigt die Internetnutzerinnen und –nutzer sind, verdächtige Webinhalte zur Anzeige zu bringen. Dank dieser Hinweise kann sich KOBIK ein besseres Bild von der Internetkriminalität in der Schweiz machen. Doch ist lediglich die Spitze des Eisbergs zu sehen. Der Grossteil des illegalen Geschehens im Internet bleibt der der breiten Öffentlichkeit verborgen. Die folgenden Ausführungen stützen sich auf Informationen aus offenen Quellen[12] und Erkenntnissen, die KOBIK in den elf Jahren ihres Bestehens sammeln konnte.

Phishing-Angriffe und zunehmend raffiniertere Betrugsmaschen

Seit den Anfängen der mithilfe des Internets begangenen Betrügereien ist einige Zeit verstrichen. Mittlerweile haben Cyberkriminelle ihre Techniken verfeinert, und ihre Vorgehensweisen zeugen von grossem Geschick. Sie beherrschen die modernen Mittel der Informatik. Dienste wie das TOR-Netzwerk, VPN-Dienste und Bulletproof-Hosting gestalten es zunehmend schwierig, Cyberkriminelle zu identifizieren. Die Schweiz ist ein wohlhabendes Land, in dem das Internet stark verbreitet ist. Nur zwei Gründe, weshalb die Schweiz auch nach 2014 ein erstrangiges Ziel für Phishing-Angriffe bleiben wird. Bei Phishing-Angriffen wird der Internetauftritt einer bekannten Einrichtung exakt nachgeahmt und ins Netz hochgeladen. Nur ausgewiesene Fachleute sind in der Lage, echte Websites von gefälschten zu unterscheiden. Um nicht von einem Antivirusprogramm entdeckt oder an einer Firewall aufgehalten zu werden, betten Cyberkriminelle diese Webseiten in Nutzerkonten von Cloud-Diensten wie Dropbox und Google Drive ein, auf die sie sich Zugriff verschafft haben. Sie verleihen so der betrügerischen Phishing-Seite den Anschein der Echtheit. Eine andere Vorgehensweise besteht darin, Schadcode in eine Webseite einzuschleusen, die ansonsten bereits einen guten Ruf geniesst. Wer solche infizierte Seiten besucht, wird unwissentlich auf eine Phishing-Seite umgeleitet. Auch hier muss damit gerechnet werden, dass der Missbrauch im Bereich von Top-Level-Domänen (z. B. *support*, *.email*) und von verfallenen oder gestohlenen Sicherheitszertifikaten[13] zunehmen wird.

Für Cyberkriminelle sind goldene Zeiten angebrochen: jeder ist mit allen und alle sind mit allen vernetzt — nicht nur am Arbeitsplatz oder zu Hause, sondern auch unterwegs. Offenbar besteht ein Bedürfnis, sich allen jederzeit mitzuteilen, sei es über die momentane Befindlichkeit oder wo man sich gerade aufhält. Betrüger machen sich das zu Nutze. Sie sammeln haufenweise Daten und Informationen, die sie zur Vorbereitung bemerkenswert ausgeklügelter Betrügereien verwenden. Vor allem die sozialen Medien dienen ihnen als Tummelplatz für ihre Gaunereien. Den Schaden tragen nicht nur die Bürgerinnen und Bürger, sondern auch die kleinen und mittleren sowie die grossen Unternehmen. Es ist zu erwarten, dass Internetbetrug und Identitätsmissbrauch im Netz noch weiter zunehmen werden.

[12] Die nachfolgend aufgeführten Internetquellen wurden jeweils zuletzt abgerufen am 18. März 2015

[13] http://www.csoonline.com/article/2687132/social-engineering/recently-introduced-tlds-create-new-opportunities-for-criminals.html

Die Schattenwirtschaft im Netz und das Darknet

Das Internet wird immer schneller, Verschlüsselungs- und Anonymisierungstechniken gewinnen zunehmend an Popularität und verbreiten sich zusehends. Mittlerweile nutzen Cyberkriminelle verstärkt auch die Vorteile, die das Darknet bietet. Am 6. November 2014 führten Europol und das FBI die Operation Onymous[14] gegen illegale Dienstleistungen im Darknet durch. Sechzehn europäische Staaten, darunter auch die Schweiz, waren daran beteiligt. Die Operation hat verdeutlicht, wie sehr neue technische Errungenschaften in weiten Kreisen der Bevölkerung verbreitet sind. Viele Geschäfte, Betriebe und Firmen verlagern ihre Tätigkeiten, nicht nur illegalen Handel, ins Darknet, das verborgene Paralleluniversum des Internets. Das Darknet bietet die Möglichkeit, mehr oder minder anonym Malware oder Daten zu Kreditkarten zu kaufen, sich ein Botnet zu mieten oder einen DDoS-Angriff durchzuführen[15]. Auf Plattformen im Darknet werden kinderpornografisches Material getauscht, illegale Betäubungsmittel und eine Vielzahl anderer verbotener Waren gehandelt. Vereinfacht wird das Ganze durch die Verwendung virtueller Währungen wie Bitcoins und Zahlungsdienstleistungen, über die Geld noch ungleich diskreter als üblich und unter Wahrung der Identität transferiert werden kann.

Es gibt kriminelle Gruppen, die sich längst nicht mehr nur darauf beschränken, Dienstleistungen zu verkaufen. Mittlerweile bieten sie ihren «Kunden» veritablen Kundendienst und Rund-um-die-Uhr-Support an[16]. Wer möchte und es sich leisten kann, mietet Botnets, um massenhaft Spam oder Trojaner zu versenden. Gibt es Anwendungsprobleme, ist der technische Support inbegriffen. Diese Kriminellen haben ein neues innovatives und konkurrenzfähiges Geschäftsmodel entwickelt: *Crime-as-a-Service.* Cyberverbrechen sind längst nicht mehr Spezialisten vorbehalten. Jeder, der das nötige Geld hat, kann mitmischen. Und alles deutet darauf hin, dass sich diese Entwicklung in den kommenden Jahren verstärkt.

Malware auf Mobiltelefonen

Dem herkömmlichen Computer wird in naher Zukunft durch Smartphone und Tablets noch weit mehr Konkurrenz erwachsen als bisher.[17] Smartphone ist ein Synonym für ständiges Verbunden- und Erreichbarsein. Bei vielen hat sich das Smartphone deshalb als Kommunikationsmittel der ersten Wahl bereits durchgesetzt. Das Smartphone ist gleichsam das Bindeglied zwischen seinem Besitzer und dessen virtueller Identität, mit einem entscheidenden Unterschied: Der Besitzer als Individuum hat eine unveräusserliche, ihn definierende Identität; sein virtueller Avatar hingegen ist ein vages Konglomerat einzelner, verstreuter und schwer kontrollierbarer Elemente wie E-Mails, Fotos, SMS oder soziale Netzwerke. Der durchschnittliche Nutzer ist sich in der Regel bewusst, wie wichtig es ist, den eigenen Computer durch laufend aktualisierte Antivirus-Programme zu schützen. Die Risiken, die Wearables[18] bergen, gehen indessen oft vergessen. Cyberkriminelle nutzen Unwissen oder Unbekümmertheit der Benutzer hemmungslos aus. Laufend wird neue Malware entwickelt, mit deren Hilfe Cyberkriminelle im Mobiltelefon gespeicherte oder im Internet verstreute Datenelemente über eine Person herausfiltern, um kostenpflichtige Dienstleistungen zu abonnieren oder gebührenpflichtige Sonder- und Servicenummern anzuwählen. All das geschieht ohne das Wissen des Besitzers des Mobiltelefons. Bislang auf den Computer beschränkte Malware findet sich mittlerweile auch in Betriebssystemen tragbarer IT-Geräte. Vergangenes Jahr wurde erstmals eine Android-Ver-

[14] https://www.europol.europa.eu/content/global-action-against-dark-markets-tor-network

[15] Trend Micro, Deepweb and Cybercrime, 2013, pp. 9 et ss.

[16] Europol, The Internet Organised Crime Threat Assessment (iOCTA) report, 2014, S.11

[17] http://www.forbes.com/sites/louiscolumbus/2013/09/12/idc-87-of-connected-devices-by-2017-will-be-tablets-and-smartphones

[18] tragbare Kleinst-IT-Geräte, wie beispielsweise Smartwatches

sion des Reveton-Trojaners entdeckt, einer Ransomware, die sich dem Nutzer als vermeintliche Warnung einer offiziellen, meist polizeilichen Institution präsentiert[19]. Auch der Bereich der virtuellen Zahlungsmittel ist von Malware nicht verschont geblieben. So kann eine Malware Smartphones dazu bringen, dass es für die Cyberkriminellen, die die Malware in Umlauf gebracht haben, Bitcoins scheffelt. Alles auf Kosten der nichts ahnenden Besitzer[20].

Altbekannte Schwachstellen, Cloud Computing und neue Zahlungssysteme

Vergangenes Jahr kam eine Reihe schwerwiegender Programmfehler (z. B. Heartbleed[21] und Shellschock[22]) und Sicherheitslücken in älteren Internet-Protokollen und Betriebssystemen zum Vorschein (z. B. POODLE[23]). Dadurch war es unter anderem möglich, Botnets einzurichten und zu verwalten[24]. In Zukunft ist mit Angriffen dieser Art ist zu rechnen und es gilt, angemessen darauf reagieren zu können.

Ein weiteres Thema: Cloud-Computing. Cloud-Dienste speichern riesige Mengen an Informationen. Diese Dienste sind denn auch beliebte Ziele von Kriminellen. Der Skandal um die unrechtmässig aus dem Online-Speicherdienst iCloud gestohlenen pikanten Aufnahmen von amerikanischen Stars und Sternchen[25] verdeutlicht, welche Folgen eine winzige Sicherheitslücke haben kann. Die Masse an Informationen, die in Clouds gespeichert sind, dürfte viele Cyberkriminelle auf den Geschmack gebracht haben und dafür sorgen, dass es in nächster Zeit zu weiteren Angriffen auf Clouds kommen wird. Die Nutzer von Cloud-Diensten tun gut daran, ihre Konten und den Zugriff darauf zu sichern, beispielsweise indem für den Zugang Zwei-Faktor-Authentifizierung und komplexe Passwörter erforderlich sind.

Apple Pay, *Google Wallet* und *Cashcloud*: Das sind die Namen nur einiger weniger Anbieter immer neuer bargeldloser Zahlungssysteme, die um die Gunst der Konsumenten wetteifern, in der Absicht, ihr System als unseren digitalen Geldbeutel von morgen zu etablieren. Wie alles Neue rufen diese Systeme auch Cyberkriminelle auf den Plan. Umso ratsamer ist es, dass die Konsumenten den sicheren Umgang mit diesen Systemen erlernen.

The Internet of Things

Cisco geht davon aus, dass bis 2020 rund 50 Milliarden Geräte und Einrichtungen des täglichen Lebens ans Internet angeschlossen sein werden[26]: Computer, Tablets, Smartphones ebenso wie Duschen, Küchen, Lampen, Thermostate, Autos und vieles mehr: The Internet of Things, oder zu Deutsch das Internet der Dinge[27]. Es ist damit zu rechnen, dass Cyberkriminelle diese Entwicklung nicht ungenutzt an sich vorbeiziehen lassen werden.

Wer sich also der Möglichkeiten bedient, die diese neuen Technologien bieten, muss sich auch der Risiken bewusst sein, die mit deren Nutzung einhergehen. Ein vernünftiger Umgang mit den Vorteilen dieser neuen Möglichkeiten und eine gesunde Priese Vorsicht sind der beste Schutz.

---

[19] http://blog.trendmicro.com/trendlabs-security-intelligence/ransomware-moves-to-mobile/

[20] https://blog.lookout.com/blog/2014/04/24/badlepricon-bitcoin/

[21] http://heartbleed.com

[22] http://www.troyhunt.com/2014/04/24/badlepricon-bitcoin/

[23] https://access.redhat.com/articles/1232123

[24] SWITCHcert Report zu aktuellen Trends im Bereich IT-Security und Privacy, November 2014, pp. 1-2

[25] http://time.com/3247717/jennifer-lawrence-hacked-icloud-leaked/

[26] SWITCHcert Report zu aktuellen Trends im Bereich IT-Security und Privacy, Oktober 2014, pp. 4-5

[27] http://postscapes.com/internet-of-things-examples/