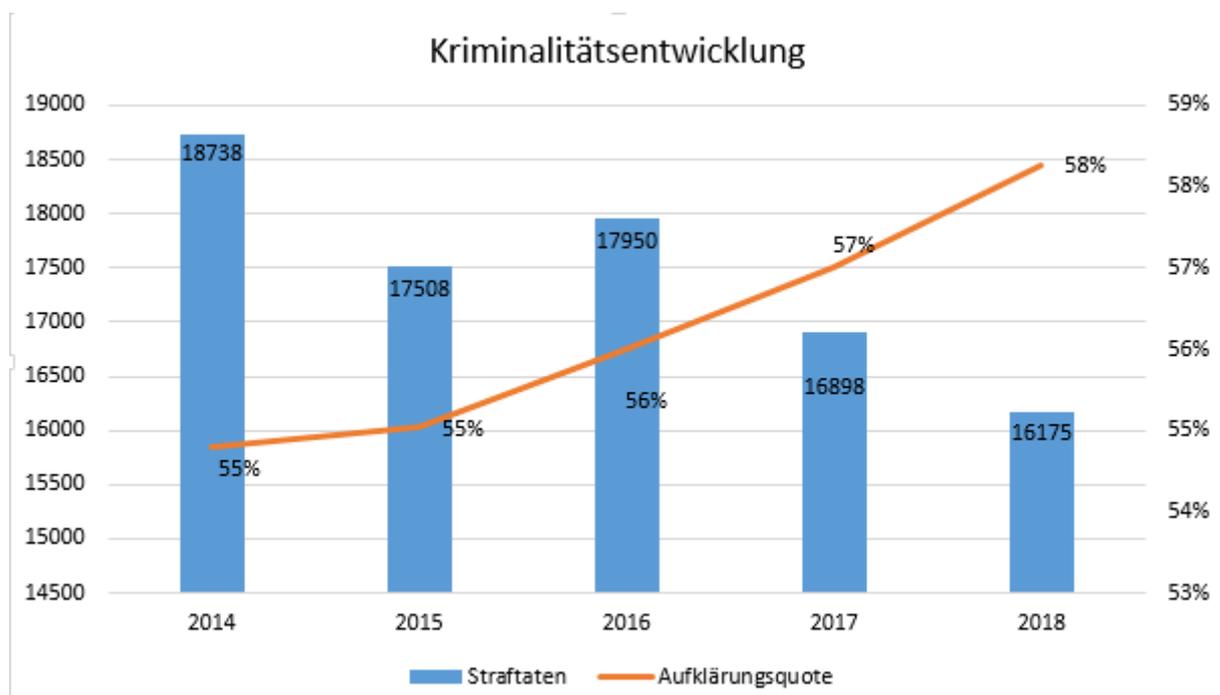
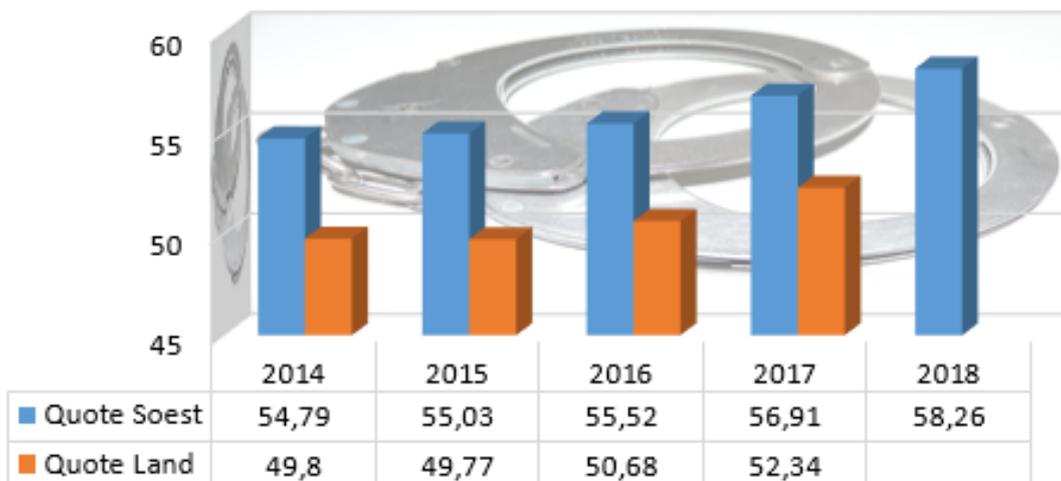
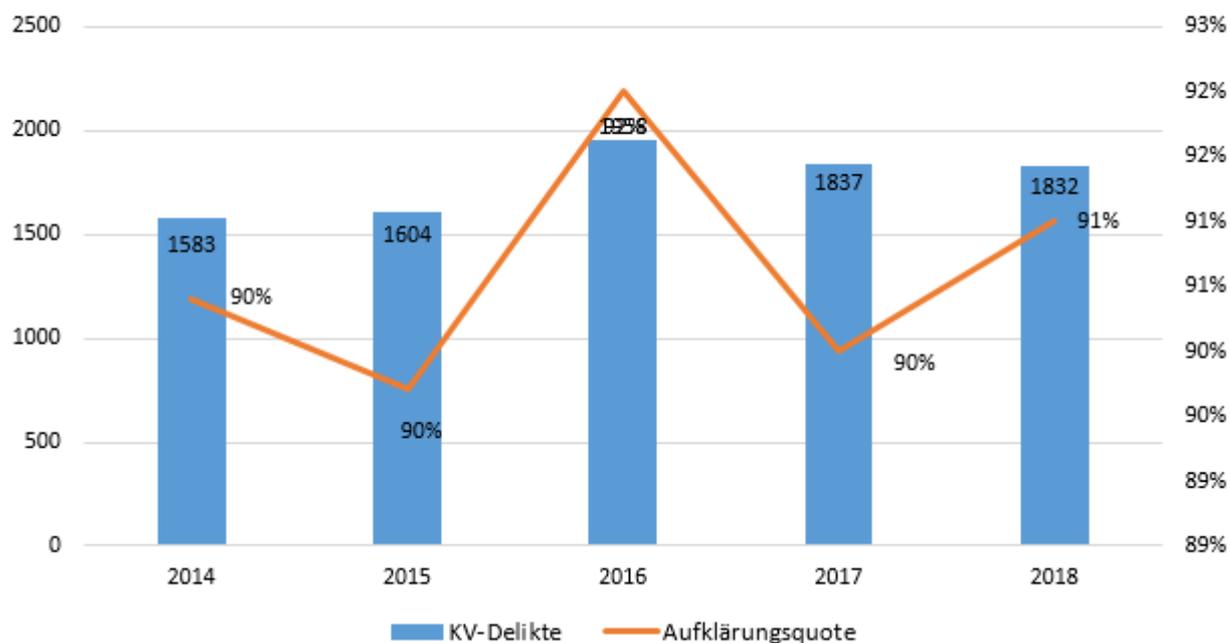


Kriminalitätsbekämpfung

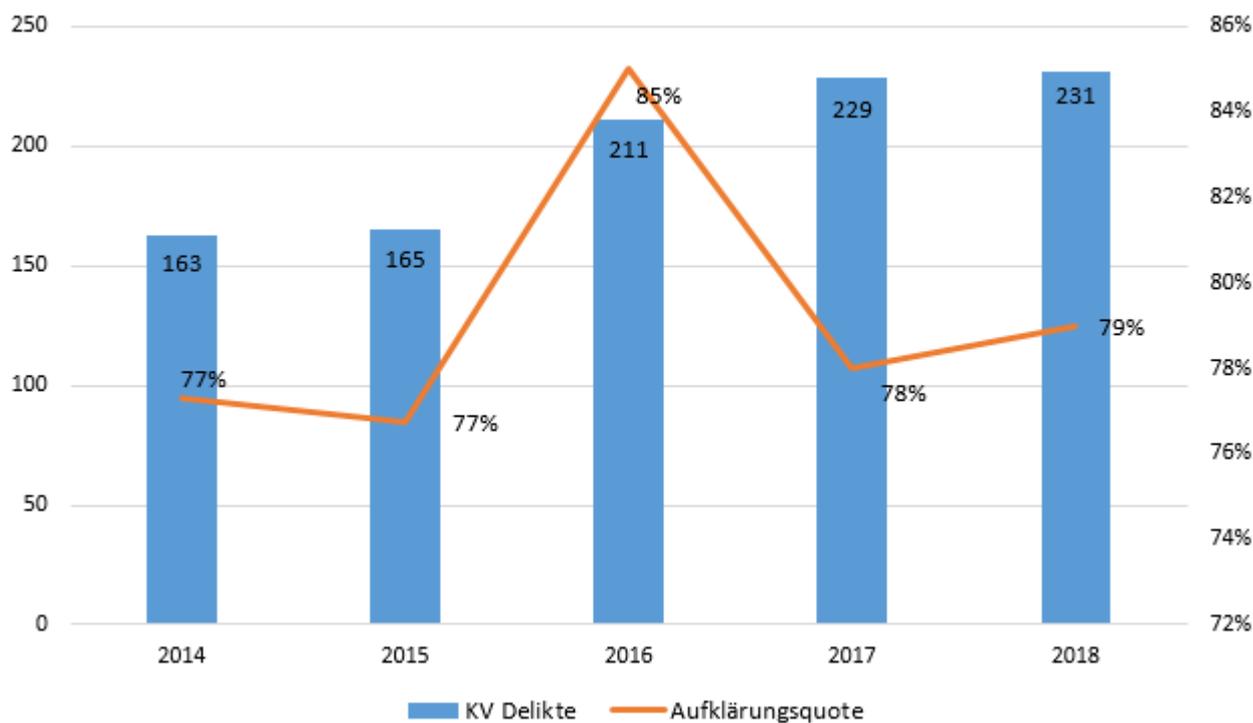
Aufklärungsquoten



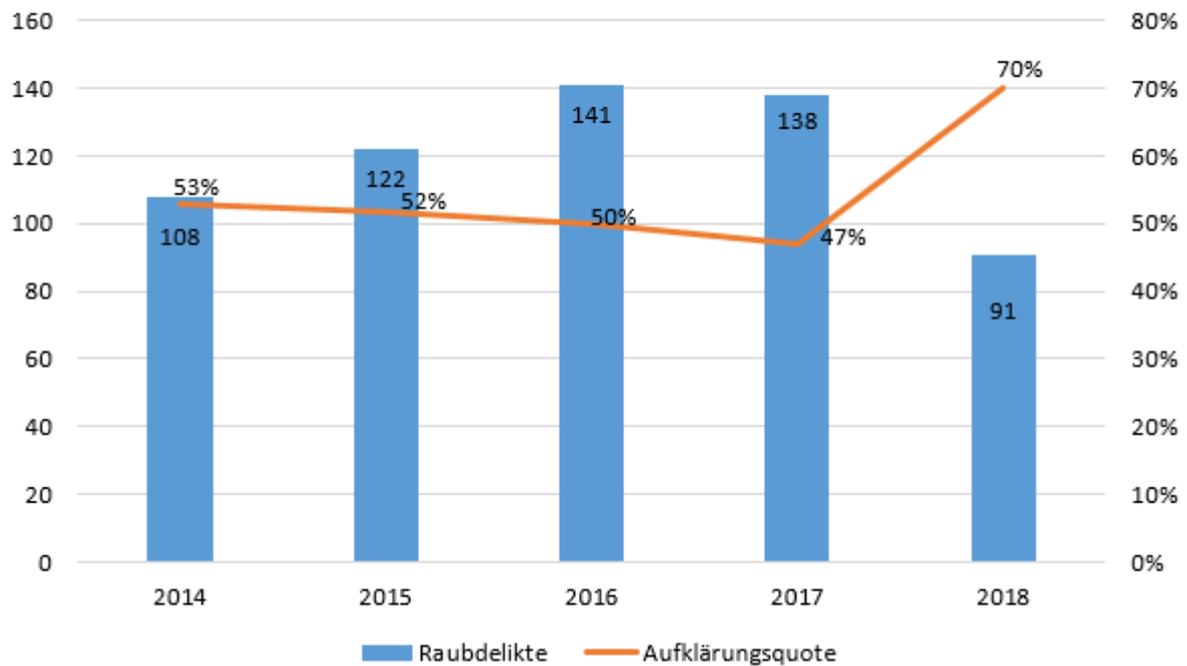
Körperverletzungsdelikte



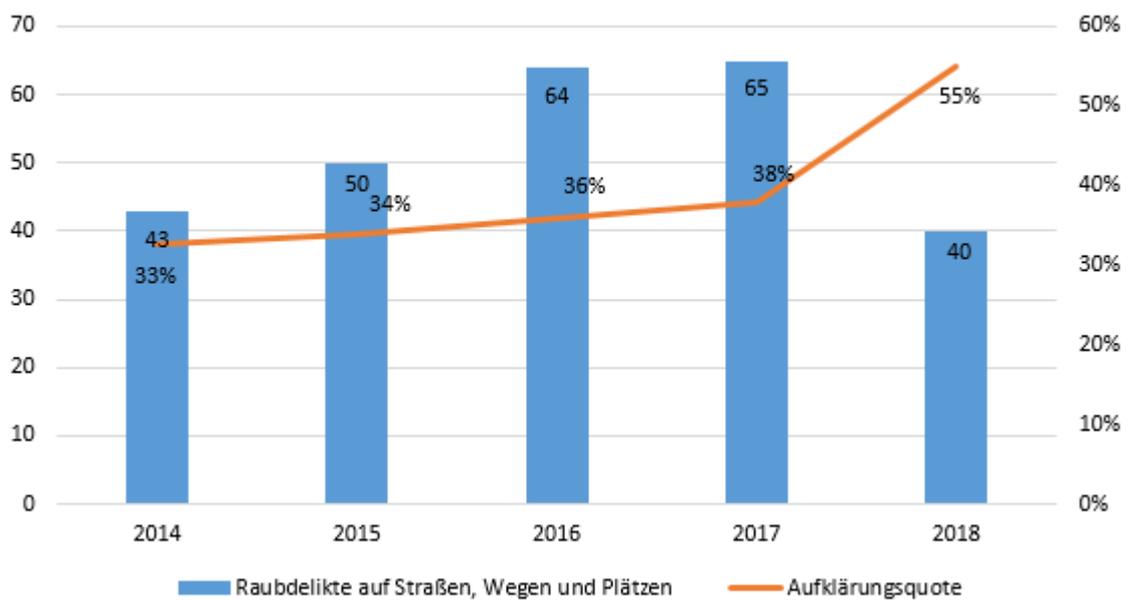
Gefährliche Körperverletzung auf Straßen, Wegen und Plätzen



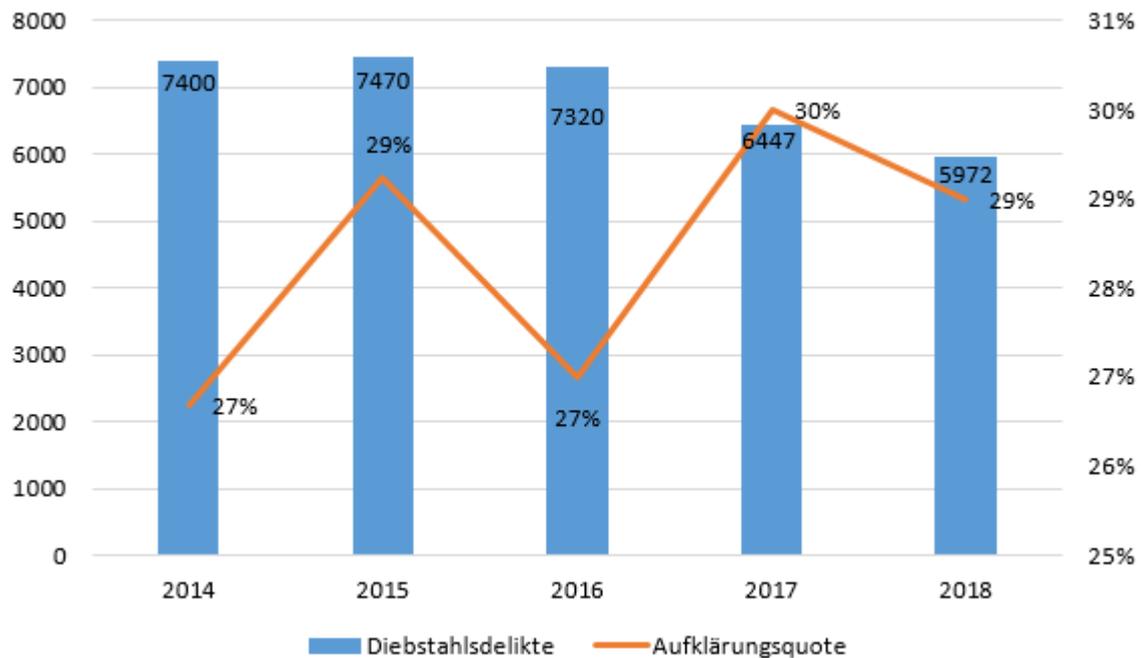
Raubdelikte



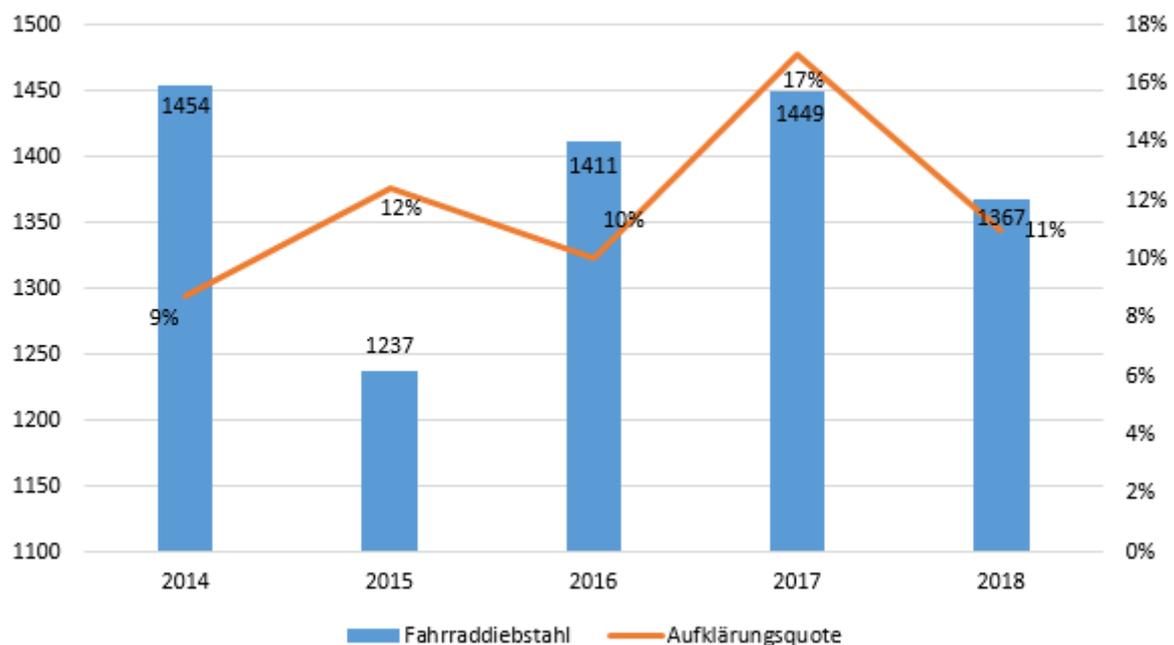
Raubdelikte auf Straßen, Wegen und Plätzen



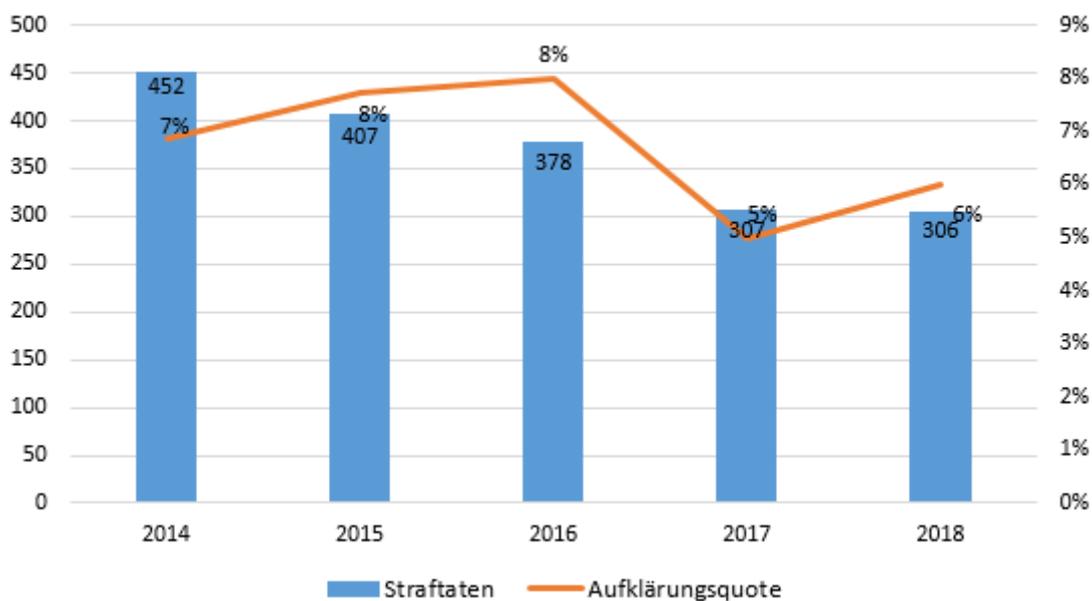
Diebstahlsdelikte



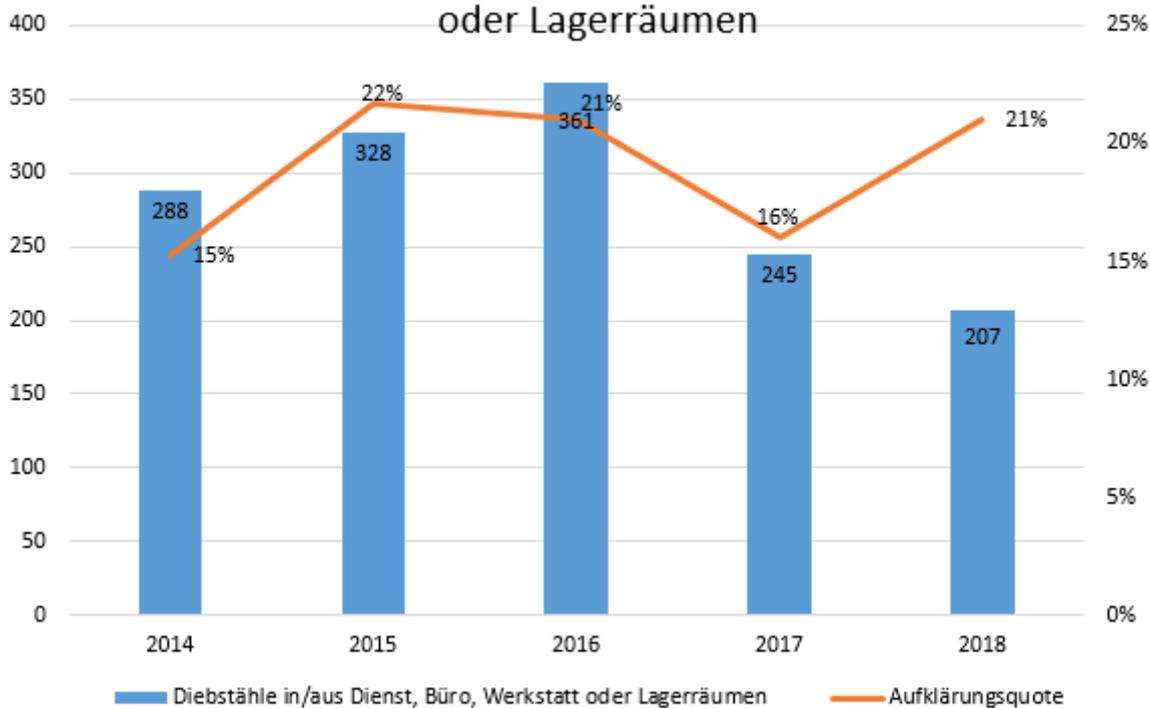
Fahrraddiebstahl



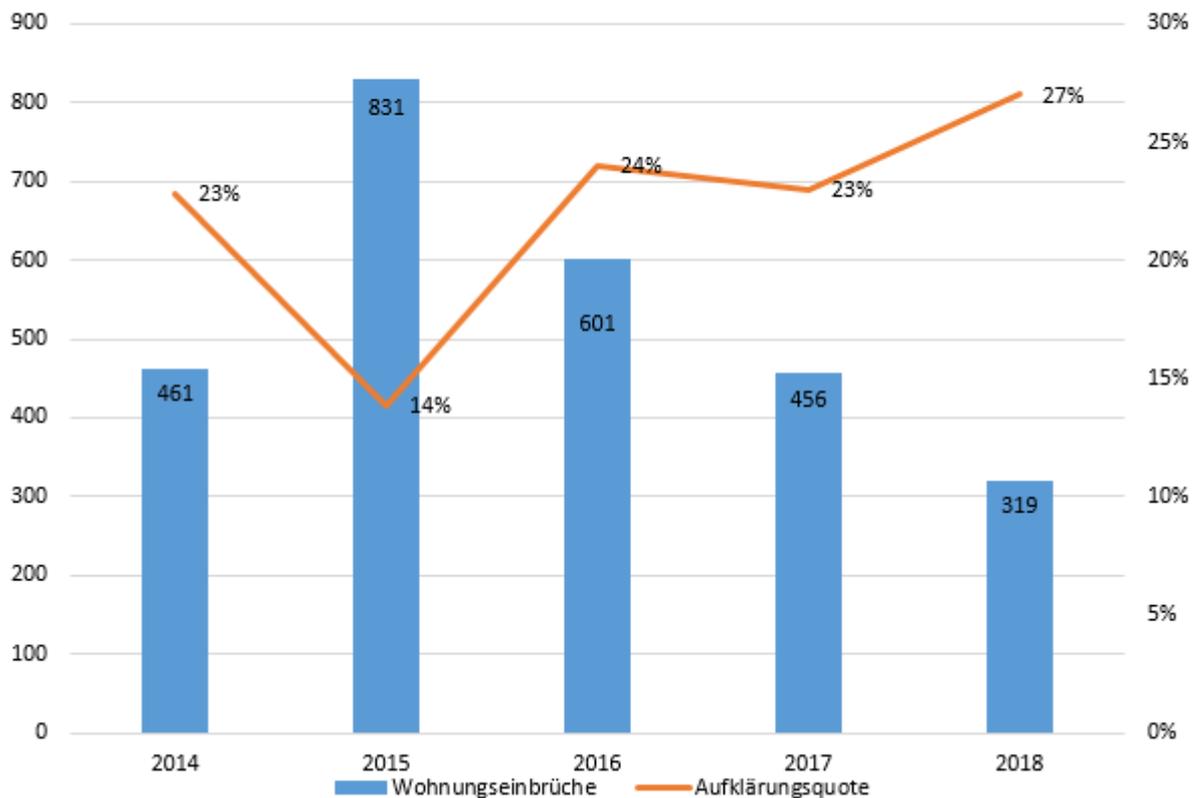
Taschendiebstahl



Diebstähle in/aus Diensträumen, Büro, Werkstatt oder Lagerräumen



Wohnungseinbrüche



Sinkende Fallzahlen bei den Wohnungseinbrüchen

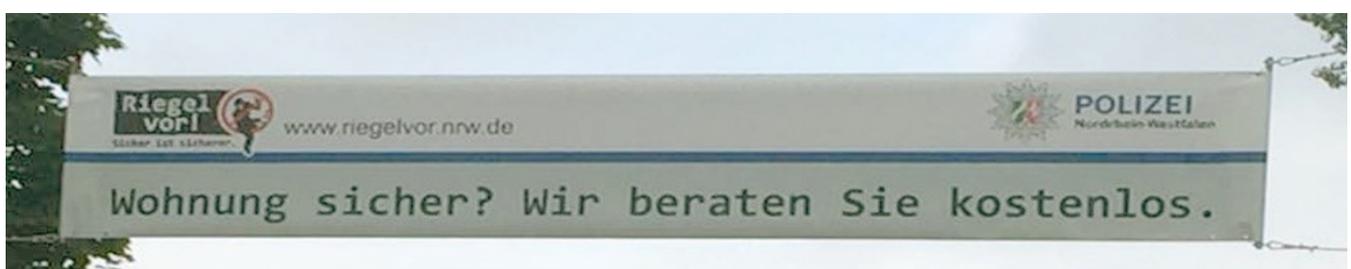
Auch wenn die Einbruchszahlen in den letzten drei Jahren stetig gesunken sind, so geht die Kreispolizeibehörde Soest noch immer mit einer Ermittlungskommission gegen die Einbrecher vor. Die EK Muräne ist seit vier Jahren fester Bestandteil der Arbeit der Kriminalpolizei.

Wenn man Opfer geworden ist ...

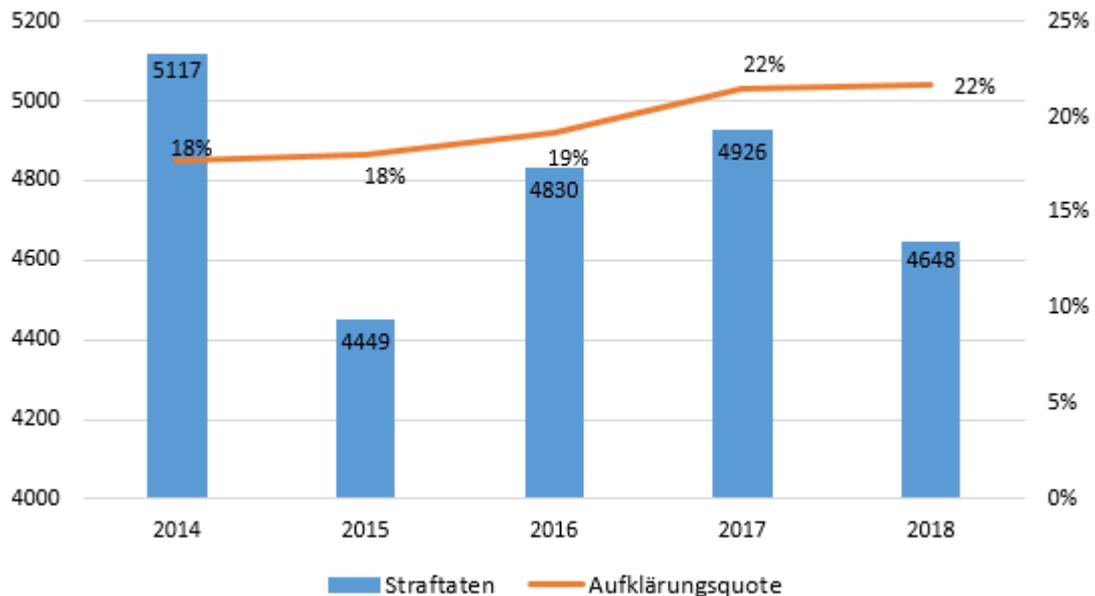
Trotz zurückgehender Zahlen im ganzen Land, sollten die Bürger weiter vorsichtig sein und die Tipps der Kriminalprävention befolgen. Für die meisten Opfer ist nicht der Verlust von Wertgegenständen, sondern das Bewusstsein, dass ein Fremder die Wohnung durchsucht hat, das Problem.

Mit einer landesweiten Aktionswoche im Herbst und den immer wieder erwähnten Hilfestellungen unserer Sicherheitsexperten wollen wir das Thema bei der Bevölkerung präsent halten.

Mit solchen Bannern wirbt die Kriminalprävention für ihre Beratung.



Straßenkriminalität



Zur Straßenkriminalität gehören Vergehen aus den Bereichen: Raub, sexuelle Übergriffe, Diebstahl, Sachbeschädigungen und Körperverletzungen.

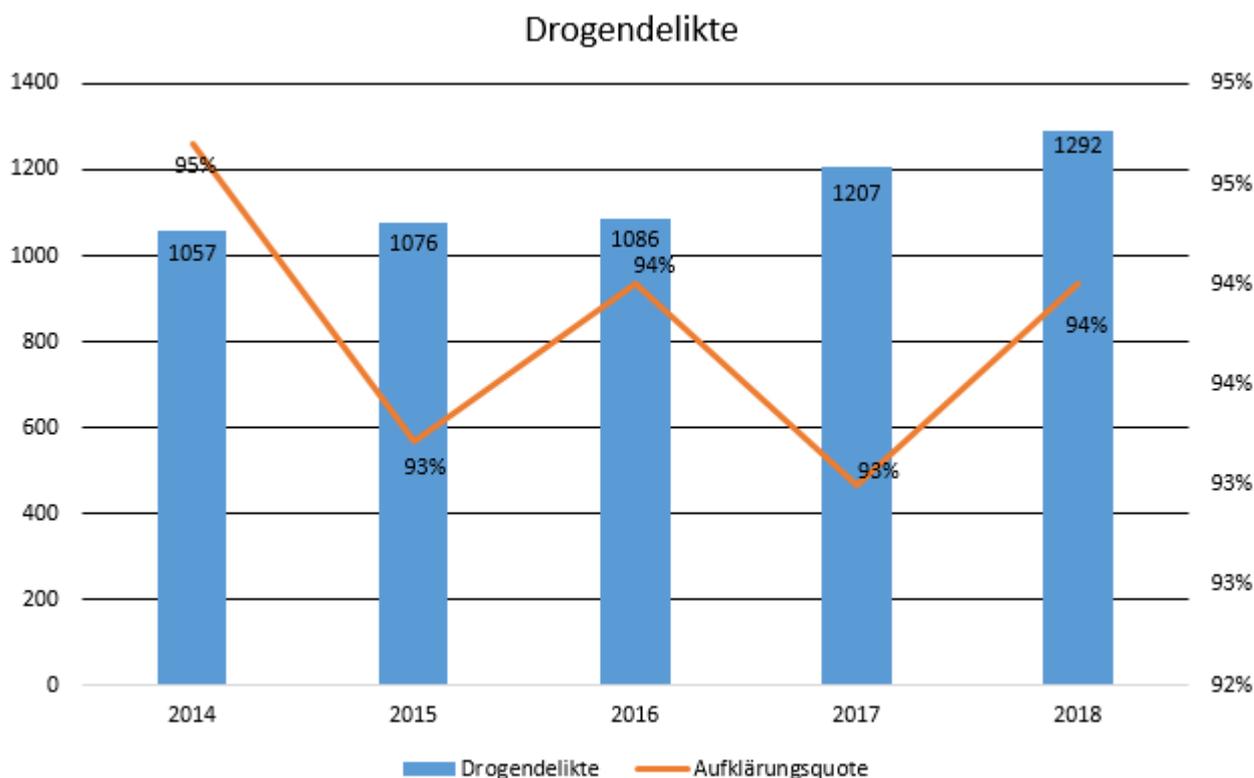
Insgesamt zählen 80 verschiedene Delikte zur Straßenkriminalität.



*Wo gefeiert wird, gibt es auch vermehrt Straftaten.
Dies gilt besonders für Großveranstaltungen.*



*Sachbeschädigen machen einen großen Teil der
Straßenkriminalität aus.*



Betäubungsmittelkriminalität ist ein typisches Kontrolldelikt. In diesem Deliktsbereich kann die Polizei nur sehr begrenzt auf Hinweise aus der Bevölkerung hoffen. Eine Veränderung der Anzahl der bekannt gewordenen Fälle weist nicht gleichzeitig auf eine positive oder negative Veränderung im „BtM-Milieu“ hin. In der Regel ist ein Anstieg der Fallzahlen im Bereich der Betäubungsmittelkriminalität auf eine Intensivierung der Ermittlungs- und Kontrolltätigkeit der Polizei zurück zu führen.

Betäubungsmitteldelikte werden bei der Kreispolizeibehörde Soest auch im Jahr 2019 weiterhin zentral im Kriminalkommissariat 3 bearbeitet.

Die intensiven Ermittlungen dieses Kommissariats führten im Jahr 2018 bei **1292 Fällen** zu einer Aufklärungsquote von **94,12 %**.

Da Abhängige harter Drogen ihre Sucht durch die Begehung von Straftaten finanzieren (sog. indirekte Beschaffungskriminalität), können durch eine intensive BtM-Sachbearbeitung auch Diebstahlsdelikte aufgeklärt oder verhindert werden.

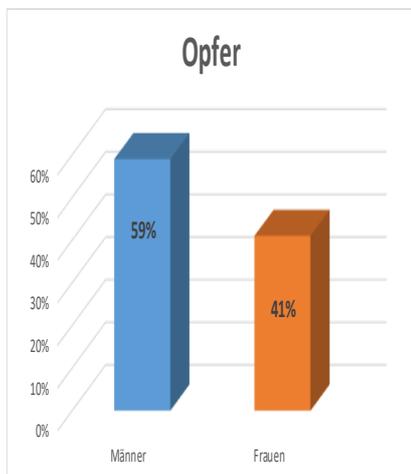
Drei Drogentote im Kreis Soest

Im Jahr 2018 wurden **357** Tatverdächtige (5,32 % der ermittelten Tatverdächtigen -gesamt) als Konsumenten harter Drogen erfasst.

Drei Erwachsene starben im Jahr 2018 aufgrund übermäßigen Drogenkonsums.

Die Opfer

In der polizeilichen Kriminalstatistik werden Opfer nur dann erfasst, wenn es sich um Straftaten handelt, die das Leben, die sexuelle Selbstbestimmung, die körperliche Unversehrtheit oder die persönliche Freiheit beeinträchtigen sowie bei Raubdelikten.



Als Opfer erfasst wurden im Jahr 2018 bei 2.949 Delikten insgesamt 3447 Menschen, davon sind 1412 weiblich (41 %) und 2035 männlich (59 %).

Die Zahl der nichtdeutschen Opfer betrug 716 (20,8 %).

Bei den unter 21 Jährigen Opfern waren 347 weiblich (40,2%) und 474 männlich (59,8%).

Opferschutz

Da Personen, die Opfer von Straftaten geworden sind, besondere Aufmerksamkeit verdienen, sind bei der Kreispolizeibehörde Soest zwei Beamte hauptamtlich im Bereich des Opferschutzes eingesetzt. Die beiden Beamten nehmen mit den Opfern Kontakt

auf, weisen auf Opferrechte hin und vermitteln im Bedarfsfall Hilfeleistungen und/oder stellen Kontakte zu Opferhilfsorganisationen her. Im Jahr 2018 wurden 635 Opfernachsorgegespräche (18,4 % der Fälle) geführt.

Häusliche Gewalt

Delikte der „Häuslichen Gewalt“, bei denen Körperverletzungsdelikte im Rahmen einer häuslichen Gemeinschaft, zum Beispiel unter Eheleuten begangen werden, erfahren bei der Polizei besondere Aufmerksamkeit.

Gewalt im „sozialen Nahraum“ ist ein Phänomen, von dem überwiegend Frauen und Kinder als Opfer betroffen sind. Obwohl sich das Anzeigeverhalten in den zurückliegenden Jahren bereits deutlich verändert hat, dürfte das Dunkelfeld erheblich sein, da gemutmaßt werden kann, dass eine Vielzahl von Straftaten nicht bei der Polizei angezeigt wird. Häusliche Gewalt ist ein gesellschaftliches Problem, an dessen Bekämpfung und Bearbeitung oftmals mehrere staatliche Stellen beteiligt sind. Regelmäßig ist die Polizei die erste staatliche Instanz vor Ort.

Bereits seit einigen Jahren stehen Delikte der Häuslichen Gewalt im besonderen Fokus der Polizei. Neben den strafrechtlichen Ermittlungen sind gefahrenabwehrende Aspekte vorrangig zu beachten. Zum Schutz vor häuslicher Gewalt sind gefahren-



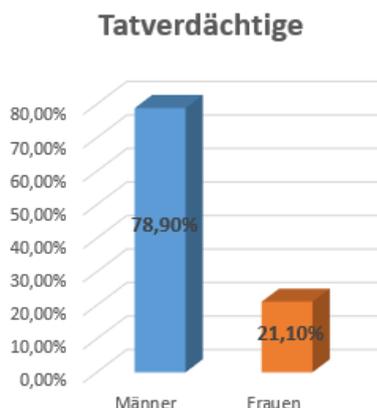
abwehrende Maßnahmen wie die Wohnungsverweisung und das Rückkehrverbot in jedem Einzelfall zu prüfen. Da innerhalb der Häuslichen Gewalt unterschiedlichste Straftatbestände berührt sein können, lässt die Polizeiliche Kriminalstatistik keine detaillierten Aussagen zur Deliktshäufigkeit zu.

Gefährderansprachen

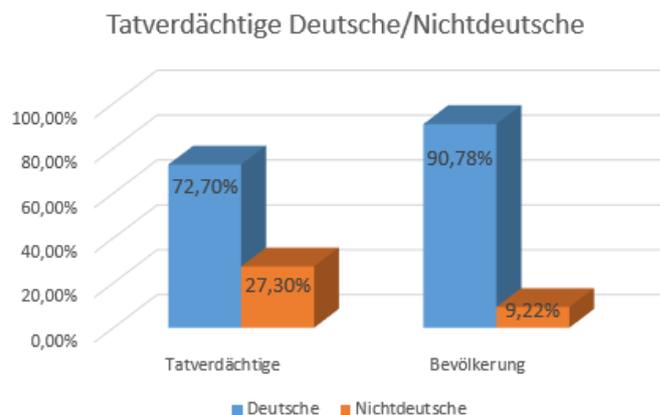
Im Jahr 2018 wurden insgesamt 486 Strafanzeigen mit Bezügen zur „Häuslichen Gewalt“ erfasst. In 332 Fällen wurden so genannte Gefährderansprachen durchgeführt, in 218 Fällen wurden gegen die Beschuldigten Wohnungsverweisungen mit einem zeitlich befristeten Rückkehrverbot ausgesprochen. 217 Geschädigte, die Opfer „Häuslicher Gewalt“ wurden, konnten durch die Kollegen des Opferschutzes an Beratungsstellen vermittelt werden.

Tatverdächtige

Von 6.707 im Jahr 2018 ermittelten Tatverdächtigen waren 78,9 % männlich und 21,1% weiblich.



Tatverdächtige überproportional häufig vertreten sind. Von den 6.707 ermittelten Tatverdächtigen handelte es sich bei 1828 um Menschen anderer Nationalitäten (Anteil 27,3%).



Tatverdächtige nach Altersgruppen alle Straftaten

Bei den insgesamt 6.707 Tatverdächtigen (TV) beträgt der Anteil der unter 21 jährigen TV 23,1 % (1.543), der männliche Anteil liegt hier bei 78,5 % (1211 TV).

Junge Menschen haben die besondere Aufmerksamkeit der Polizei im Kreis Soest. Es wird angestrebt, sie als mögliche Opfer vor Straftaten zu schützen, aber auch zu verhindern, dass sie straffällig werden. Die Delinquenz dieser Altersgruppe geht über die typischen Delikte wie Diebstähle, Körperverletzungen und Sachbeschädigungen hinaus bis in den Verkehrsbereich, wo sie mit Aggressions- und Leichtsinnsdelikten im Straßenverkehr auffallen.

Tatverdächtige Deutsche/Nichtdeutsche

Im Kreis Soest werden weitaus mehr Straftaten von Deutschen als von Bürgern anderer Nationalität begangen. In etwa 72,7 % der Fälle wurden Deutsche als Tatverdächtige ermittelt.

Unter Berücksichtigung des jeweiligen Anteils der Deutschen und Nichtdeutschen an der Bevölkerung, ist allerdings feststellbar, dass nichtdeutsche

Der Anteil der im Kreis Soest gemeldeten ausländischen Mitbürger beträgt 9,22 %.

Tatverdächtige und Alkohol

Von den 6.707 ermittelten Tatverdächtigen standen 972 Tatverdächtige unter Alkoholeinfluss (14,5 %). Der Anteil der männlichen alkoholisierten Tatverdächtigen betrug dabei 91,4 %.

Bei den gefährlichen Körperverletzungsdelikten auf Straßen, Wegen oder Plätzen betrug der Anteil der alkoholisierten Tatverdächtigen nahezu 38 %.



Erpressung Tatmittel Internet

Historie

Die Entwicklung von Ransomware, mit welcher PC's verseucht oder verschlüsselt werden, begann bereits im Jahr 1972. Anfänglich wurde Hardware wie z.B. Disketten infiziert, später wurde auch Software, beispielsweise Spiele, mit Trojanern oder Viren verseucht. Heutzutage erfolgt die Infektion eines Rechners fast ausschließlich über das Internet, sei es über infizierte Seiten, Internetportale oder infizierte Dateianhänge.

Bei „AIDS“ im Jahr 1989 handelte es sich um den ersten dokumentierten Erpressungstrojaner, welcher über eine präparierte Diskette Computer komplett verschlüsselte. Einer der

hier bekanntesten Trojaner wurde Anfang 2013 festgestellt. Der sogenannte „**BJA Trojaner**“ täuschte über einen Sperrbildschirm den Nutzern vor, dass auf ihren Rechnern kinderpornografisches Material gefunden worden wäre und gegen Zahlung einer Geldsumme die Entsperrung des PC erfolgen könne.

In der Folge wurden weitere Trojaner wie **CryptoLocker**, **Ginx**, **Locky** oder **WannaCry** bekannt. „WannaCry“ war so aggressiv ausgelegt, dass über das Rechenzentrum die gesamte digital Infrastruktur beispielsweise eines Krankenhauses zum Erliegen kam.

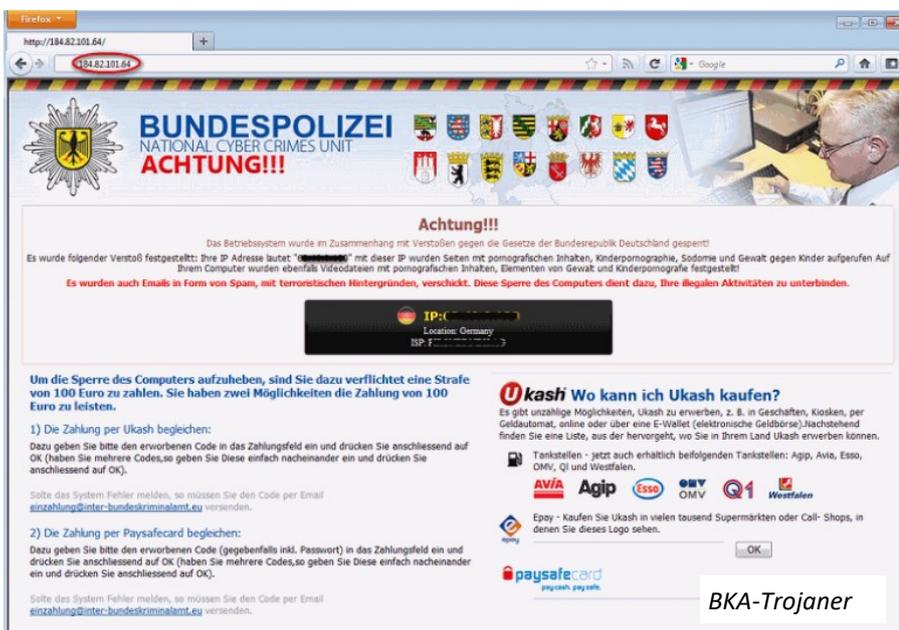
Die Bezahlung für die Entschlüsselung der PC's beziehungsweise der Dateien wird meist über Ukash, Paysafecard, iTunes -

Cards oder auf ein Bitcoin Konto gefordert.

Nach Zahlung der geforderten Summe ist es tatsächlich nur in wenigen Fällen auch zur Entsperrung der Rechner gekommen.

Ransomware: Phänomenbeschreibung

Ransomware ist eine Malware, die den Computer infiziert, sperrt und dann Geld für die Entsperrung verlangt. Die Einschleusung des Schadprogramms erfolgt auf unterschiedliche Weise. E Mail Anhang, schädliche Links, Exploit Kits (beim Besuch infizierter Webseiten oder beim Anklicken auf infizierte Werbeanzeigen von unschädlichen Webseiten). Sobald eine Lücke gefunden wird, lädt das Exploit Kit die Ransomware herunter und installiert sie auf dem Computer, was der Geschädigte in den meisten Fällen nicht merkt. Die Dateien auf dem Computer werden verschlüsselt und im Prinzip die Inhalte einer Datei chiffriert. Um die Dateien korrekt zu dechiffrieren benötigt man einen Schlüssel, für welchen die Erpresser eine Art Lösegeld verlangen.



BUNDESPOLIZEI
NATIONAL CYBER CRIMES UNIT
ACHTUNG!!!

Achtung!!!
Das Betriebssystem wurde im Zusammenhang mit Verstößen gegen die Gesetze der Bundesrepublik Deutschland gesperrt!
Es wurde folgender Verstoß festgestellt: Ihre IP Adresse lautet: "184.82.101.64" mit dieser IP wurden Seiten mit pornografischen Inhalten, Kinderpornografie, Sodomie und Gewalt gegen Kinder aufgerufen auf Ihrem Computer wurden ebenfalls Videodateien mit pornografischen Inhalten, Elementen von Gewalt und Kinderpornografie festgestellt!
Es wurden auch Emails in Form von Spam, mit terroristischen Hintergründen, verschickt. Diese Sperre des Computers dient dazu, Ihre Regalen Aktivitäten zu unterbinden.

IP-Adresse
Location: Germany
ISP: F...

Um die Sperre des Computers aufzuheben, sind Sie dazu verpflichtet eine Strafe von 100 Euro zu zahlen. Sie haben zwei Möglichkeiten die Zahlung von 100 Euro zu leisten.

1) Die Zahlung per Ukash begleichen:
Dazu geben Sie bitte den erworbenen Code in das Zahlungsfeld ein und drücken Sie anschließend auf OK (haben Sie mehrere Codes, so geben Sie Diese einfach nacheinander ein und drücken Sie anschließend auf OK).

Sollte das System Fehler melden, so müssen Sie den Code per Email einzahlung@inter-bundeskriminalamt.eu versenden.

2) Die Zahlung per Paysafecard begleichen:
Dazu geben Sie bitte den erworbenen Code (gegebenfalls inkl. Passwort) in das Zahlungsfeld ein und drücken Sie anschließend auf OK (haben Sie mehrere Codes, so geben Sie Diese einfach nacheinander ein und drücken Sie anschließend auf OK).

Sollte das System Fehler melden, so müssen Sie den Code per Email einzahlung@inter-bundeskriminalamt.eu versenden.

Ukash Wo kann ich Ukash kaufen?
Es gibt unzählige Möglichkeiten, Ukash zu erwerben, z. B. in Geschäften, Kiosken, per Geldautomat, online oder über eine E-Wallet (elektronische Geldbörse). Nachstehend finden Sie eine Liste, aus der hervorgeht, wo Sie in Ihrem Land Ukash erwerben können.

Tankstellen - jetzt auch erhältlich befolgenden Tankstellen: Agip, Avia, Esso, OMV, Q1 und Westfalen.

Epay - Kaufen Sie Ukash in vielen tausend Supermärkten oder Call-Shops, in denen Sie dieses Logo sehen.

BKA-Trojaner

Beschreibung des Phänomens

Vermeintlich erhalten Geschädigte E-Mails von unbekanntem Tätern meist in englischer Sprache, welche diese so verändern, dass sie den Anschein erwecken, der Mail-Account der Geschädigten wurde „gehackt“. Als Absender Mail-Adresse wird den Geschädigten in den meisten Fällen ihre eigene E-Mail-Adresse angezeigt. In diesen E-Mails wird den Nutzern vorgetäuscht, der PC sei gehackt und dabei festgestellt worden, dass sie intime Seiten besucht hätten.

Teilweise habe man die angeblich besuchten Seiten per Screenshot oder auch Aufnahmen über die Webcam gesichert, welche die Nutzer bei angeblichen sexuellen Handlungen vor dem Bildschirm zeigten. Für die angebotene Diskretion und eine damit verbundene Nichtweitergabe an Freunde und Bekannte, werden unterschiedlich hohe, meist dreistellige Euro-Beträge, gefordert.



Ich grüße Sie!

Beispiel

Ich habe schlechte Nachrichten für dich.

28.06.2018 - an diesem Tag habe ich Ihr Betriebssystem gehackt und vollen Zugriff auf Ihr Konto erhalten@....de

Wie war es:

In der Software des Routers, mit der Sie an diesem Tag verbunden waren, gab es eine Sicherheitsanfälligkeit.

Ich habe diesen Router zuerst gehackt und meinen bösartigen Code darauf abgelegt. Bei der Eingabe im Internet wurde mein Trojaner auf dem Betriebssystem Ihres Geräts installiert.

Danach habe ich alle Daten auf Ihrer Festplatte gespeichert (ich habe Ihr gesamtes Adressbuch, den Verlauf der angezeigten Websites, alle Dateien, Telefonnummern und Adressen aller Ihrer Kontakte).

Ich wollte dein Gerät sperren. Und benötigen Sie eine kleine Menge Geld für das Entsperren.

Aber ich habe mir die Websites angesehen, die Sie regelmäßig besuchen, und kam zu dem großen Schock Ihrer Lieblingsressourcen.

Ich spreche von Websites für Erwachsene. Ich möchte sagen - du bist ein großer Perverser. Sie haben ungezügelt Fantasie!

Danach kam mir eine Idee in den Sinn.

Ich habe einen Screenshot der intimen Website gemacht, auf der Sie Spaß haben (Sie wissen, worum es geht, oder?).

Danach nahm ich Ihre Freuden ab (mit der Kamera Ihres Geräts). Es stellte sich wunderbar heraus, zögern Sie nicht.

Ich bin fest davon überzeugt, dass Sie diese Bilder Ihren Verwandten, Freunden oder Kollegen nicht zeigen möchten.

Ich denke, 368€ sind ein sehr kleiner Betrag für mein Schweigen. Außerdem habe ich viel Zeit mit dir verbracht!

Ich akzeptiere nur Bitcoins.

Meine BTC-Geldbörse: 18Pt4B7Rz7Wf491FGQHPSfDeKRqnkyrMo6

Sie wissen nicht, wie Sie die Bitcoins senden sollen? Schreiben Sie in einer Suchmaschine "wie Sie Geld an die BTC-Geldbörse senden". Es ist einfacher als Geld an eine Kreditkarte zu senden!

Für die Bezahlung gebe ich Ihnen etwas mehr als zwei Tage (genau 50 Stunden). Keine Sorge, der Timer startet in dem Moment, in dem Sie diesen Brief öffnen. Ja, ja .. es hat schon angefangen!

Nach Zahlungseingang zerstören sich meine Viren und schmutzigen Fotos automatisch.

Wenn ich die angegebene Menge nicht von Ihnen erhalte, wird Ihr Gerät gesperrt, und alle Ihre Kontakte erhalten ein Foto mit Ihren "Freuden".

Ich möchte, dass du umsichtig bist.

- Versuchen Sie nicht, mein Virus zu finden und zu zerstören! (Alle Ihre Daten sind bereits auf einen Remote-Server hochgeladen.)

- Versuchen Sie nicht, mich zu kontaktieren (Dies ist nicht möglich, ich habe Ihnen diese E-Mail von Ihrem Konto aus gesendet).

- Verschiedene Sicherheitsdienste helfen Ihnen nicht weiter; Auch das Formatieren einer Festplatte oder das Zerstören eines Geräts ist nicht hilfreich, da sich Ihre Daten bereits ...

Internetkopfzeilen

```
Received: from smtp-pps-1.alg.polizei.nrw.de (1.6.112.1) by
500PAAA70EXC003.polizei.nrw.de (1.4.101.223) with Microsoft SMTP Server (TLS)
id 14.3.408.0; Wed, 6 Feb 2019 10:37:50 +0100
Received: from pps.filterd (smtp-pps-1.alg.polizei.nrw.de [127.0.0.1])      by
smtp-pps-1.alg.polizei.nrw.de (8.16.0.27/8.16.0.27) with SMTP id
x169UAkg123759 for <wolfgang.lueckenkemper@polizei.nrw.de>; Wed, 6 Feb 2019
10:37:49 +0100
```

Erweiterter oder Full-Header einer E-Mail

Insgesamt sind hier etwa vier Din A4 Seiten Metadaten vorhanden.

Die Erpresser E-Mails werden durch die Täter wahllos an ihnen bekannt gewordene Adressen versendet, in der Hoffnung, dass einige der Geschädigten Zahlungen leisten, weil sie fürchten, im Bekanntenkreis bloßgestellt zu werden. Die Erlangung von Mail-Adressen erfolgt auf unterschiedlicher Weise. Teils werden diese auf unsicheren Mail-Accounts abgegriffen, in einschlägigen Plattformen/Foren angekauft oder aus sozialen Netzwerken/Homepages abgelesen.

Tatsächlich fanden entgegen der Behauptungen in den Mails keinerlei Zugriffe auf den PC oder den E-Mail Account der Geschädigten statt.

Eine Veränderung der Anzeige in der Absender Zeile, womit den Geschädigten eine Glaubwürdigkeit untermauert werden soll, ist ohne großen Aufwand über frei

zugängliche Programme / Tools im Internet möglich.

Ermittlungsmöglichkeiten

Als Ermittlungsmöglichkeit dient hier die vom Täter versandte original E-Mail. Dies setzt voraus, dass die Geschädigten die Mail, welche in den meisten Fällen nicht mit Schadsoftware versehen ist, nicht löschen. Einer Installation von Schadsoftware, in einer Mail angehängt, oder in Links versteckt, entgeht man, indem man die Anhänge nicht öffnet bzw. nicht auf dortige Links klickt.

Über den erweiterten Kopf (Full Header) dieser E-Mails können Informationen für weitere Ermittlungsmöglichkeiten in Erfahrung gebracht werden. Beispielsweise kann aus diesem die IP-Adresse des Endgerätes der versandten Mail festgestellt werden, wenn auch erfahrungsge-

mäß der dazugehörige Server meist im Ausland steht.

Weiterhin wird aus dem Full-Header meist die tatsächliche Absende Mail Adresse sowie der Internetanbieter, wo diese Adresse angelegt wurde, ersichtlich.

Aktuell häufen sich die hier angezeigten Fälle, wobei die Dunkelziffer weitaus höher liegen dürfte.



Rainer Uebach

Kriminalhauptkommissar