Betrug und seine Bekämpfung

Gifhorn/Berlin/Brüssel (D). Die Betrugsmaschen werden immer perfider und ausgeklügelter. Vom Tod von Angehörigen über Drohungen angeblicher Anzeigen bei Staatsanwaltschaften, vom Gefühlen an Mitmenschlichkeit bis zum „bloßen“ Diebstahl materieller Güter händisch bis elektronisch ist heute alles bei der Betrugskriminalität zu finden. Auch in Brüssel beschäftigen sich die Gremien mit Betrugsmaschen, die seit Einführung und Weiterentwicklung der Smartphones und des Internets stattfinden. Am 15.12.25 legte die EU ihre Betrugsbekämpfungsarchitektur dieses Kriminalitätsfeldes offen.

Um deutlich zu machen, um was für Straftaten es sich häufig handelt und wie pervers und abgebufft die Betrüger vorgehen, hier einige Beispiele, um an denen lernen zu können:

Beispiel 1: Leer, Lk. Emsland
Am 25.11.25 kam es in der Zeit von 10:00 h bis 14:00 h zu einem Schadenseintritt nach einem Schockanruf zum Nachteil eines 65-jährigen Mannes. Der Verlauf der Tat über mehrere Stunden zeigt wieder einmal die Gefährlichkeit der Anrufe, in denen die Täter Angst und Schrecken verbreiten, die Opfer unter Druck setzen und drangsalieren. Die Täter sind Profis und auch in der Lage, am Telefon Szenarien herzustellen, die für die Opfer echt wirken. In der Panik, dass einem geliebten Menschen etwas Furchtbares widerfahren ist, verschwimmen Fiktion und Realität und die Situation wird als real empfunden. Im aktuellen Fall erfolgte der telefonische Erstkontakt über die Festnetznummer des Opfers. Hier wurde der Betrug von einer angeblichen Polizeibeamtin mit der bekannten Schockanrufgeschichte eingeleitet.

Auch hier war es die angebliche Tochter des Opfers, die einen schweren Unfall verursacht und dabei eine schwangere Frau getötet haben soll. Im weiteren Verlauf gab sich dann einer der Betrüger als Staatsanwalt aus. Er drohte dem Opfer mit einer mehrjährigen Haftstrafe für die Tochter und verlangte eine höhere fünfstellige Summe als Kaution. Zudem gelang es den Betrügern, an die Mobiltelefonnummer des Opfers zu kommen und damit den Druck dauerhaft aufrecht zu erhalten. So begleitete der Anrufer das Opfer auch zur Bank und zum anschließenden Übergabeort in Papenburg. Der Schaden liegt bei mehr als 20.000 Euro. Der Übergabeort wurde zuerst mit der Adresse des Amtsgerichtes Papenburg angegeben, wohl um mit der Adresse die Richtigkeit des Anrufes zu untermauern. Während der Fahrt wurde der Betroffene fernmündlich über sein Mobiltelefon an eine Adresse in der Nähe des Marienkrankenhauses/VHS geleitet. Dort erfolgte die Übergabe an eine männliche Person um 13:52 h. Auffällige Beobachtungen und Hinweise können an die Dienststellen in Leer gegeben werden.

Beispiel 2: Ludwigshafen (RP)
Am 12.12.25 zwischen 10:00 h und 12:36 h kam es in Ludwigshafen mehrfach zu einem sogenannten Call-Center-Betrug. Die 92-Jährige und der 93-jährige Geschädigte wurden insgesamt vier Mal über eine unterdrückte Telefonnummer auf dem Festnetztelefon angerufen. Innerhalb des Telefonats gab sich der unbekannte Täter als Amazon-Mitarbeiter aus und teilte mit, dass eine Geldsumme in Höhe von 799,00 EUR vom Konto der beiden Geschädigten abgebucht werden würde. Zu einem tatsächlichen Schaden kam es nicht.

Die Polizei weist ausdrücklich darauf hin, dass diese Betrugsversuche oft sehr professionell und glaubhaft wirken.
Die Täter bauen gezielt psychologischen Druck auf, um die Opfer zu überrumpeln. Sie verwenden oft gefälschte Telefonnummern, die auf dem Display wie eine offizielle Rufnummer der Polizei oder einer anderen Behörde aussehen. Sollten Sie einen solchen Anruf erhalten, informieren Sie Ihre örtlich zuständige Polizeidienststelle über den Sachverhalt und bitten Sie ausdrücklich um schnelle Hilfe.

Beispiel 3: Limburgerhof (RP)
Die Polizei Schifferstadt möchte Sie daraufhin hinweisen, dass es aktuell in Limburgerhof vermehrt zu Anrufen kommt, bei denen sich unbekannte Personen als Polizeibeamte ausgeben. Mit geschickter Gesprächsführung verunsichern und manipulieren sie ihre Opfer, dass sie teilweise hohe Geldbeträge und Wertgegenstände an die Täter überweisen oder sogar persönlich übergeben. Deshalb benötigen wir jetzt Ihre Mithilfe! Haben Sie gerade in ihrem Ortsbereich etwas Ungewöhnliches beobachtet? Kam Ihnen gerade etwas komisch vor? Haben Sie den Verdacht, dass in Ihrem Umfeld ein solcher Betrugsfall aktuell stattfinden könnte? Dann verständigen Sie bitte umgehend die Polizei!

Wichtiger Hinweis:
Behörden wie Staatsanwaltschaften, Gerichte oder die Polizei schicken bei Präventionsmaßnahmen oder Verfügungen diese immer und nur per Post, ein direktes sofortiges Handeln ist somit nicht erforderlich. Die Polizei gibt hier folgende Verhaltenstipps:- Geben Sie am Telefon keine Auskunft über Ihre per-

sönlichen und finanziellen Verhältnisse oder andere sensible Daten.
- Öffnen Sie unbekannten Personen nicht die Tür. Ziehen Sie gegebenenfalls eine Vertrauensperson hinzu, z. B. Nachbarn oder nahe Verwandte.
- Übergeben Sie unbekannten Personen kein Geld oder Wertsachen.

Beispiel 4: Kaiserslautern (RP)
Erneut haben Betrüger versucht, ein Ehepaar aus Kaiserslautern hereinzulegen. Wie die Frau der Polizei mitteilte, erhielt sie am Mittwoch einen Anruf eines Mannes, der sich als Mitarbeiter eines Online-Bezahldienstes ausgab.
Der Anrufer behauptete, Hacker hätten über das Konto der Frau Kryptowährungen gekauft. Auch das Konto ihres Mannes sei betroffen. Um eine Abbuchung zu verhindern, sollte das Ehepaar mehrere Apps herunterladen. Damit gewährten sie den Betrügern Zugriff auf ihre Endgeräte. Dem Paar fiel der Betrug rechtzeitig auf und sie erstatteten Anzeige. Ein finanzieller Schaden ist nicht entstanden.

Lassen Sie sich am Telefon auf keinen Fall unter Druck setzen oder zu kurzfristigen Entscheidungen verleiten- egal, wie plausibel eine Situation zunächst dargestellt wird. Geben Sie auch keine persönlichen Daten an Unbekannte heraus.

Es wird hier dringend darauf hingewiesen, sich auf das geltende deutsche Recht zu besinnen.

Sollten Betroffene einen Anruf kommen, in welchem Straftaten behauptet oder Schreckensszenarien heraufbeschworen werden, sollte sofort aufgelegt werden. Betroffene sollten sich in keinem Fall auf ein längeres Telefonat einlassen, sondern auflegen und als erstes die Familie oder andere nahestehende Personen über das Geschehen informieren und den Vorfall mit diesen aufklären. Niemals Geld an fremde Personen aushändigen, egal was diese behaupten oder androhen. Informieren Sie die örtliche Online-Wache oder das Landeskriminalamt.

Deshalb benötigen wir jetzt Ihre Mithilfe! Haben Sie gerade im Bereich Ort etwas Ungewöhnliches beobachtet? Kam Ihnen gerade etwas komisch vor? Haben Sie den Verdacht, dass in Ihrem Umfeld ein solcher Betrugsfall aktuell stattfinden könnte? Dann verständigen Sie bitte umgehend die Polizei!

Beispiel 5: Verden (NI)
Am 22.12.25 kam es in Verden zu zahlreichen Anrufen von falschen Polizeibeamten. Sie gaben sich dabei u. a. als Kriminalpolizei aus und erzählten eine Legende über eine Einbrecherbande in der Nachbarschaft und fragten nach Wertgegenständen, welche man nun schützen wolle. Viele Angerufene erkannten die Betrugsmasche oder wurden misstrauisch und beendeten daraufhin richtigerweise das Telefonat. In zwei Fällen waren die Betrüger mit ihrer Geschichte jedoch überzeugend genug.
Im Borsteler Trift und in der Rheinstraße tauchte zwischen 17:00 h und 18:00 h nach den Telefonaten ein angeblicher Polizeibeamter bei den Geschädigten auf und ließ sich die Wertgegenstände zeigen. Im Verlauf konnte der Mann die Wertgegenstände in einem unbeobachteten Moment an sich nehmen und die Tatorte wieder verlassen. Den Geschädigten fiel der Diebstahl erst anschließend auf.

Beispiel 6: Hooksiel (NI)
Am 16.10.25, kam es zwischen 11:00 h und 15:17 h in Hooksiel zu Schock-anrufen.
Eine 80-jährige Geschädigte erhielt mehrere Anrufe einer vermeintlichen Polizistin, die ihr mitteilte, dass die Tochter ihres verstorbenen Lebensgefährten in Schleswig-Holstein einen schweren Verkehrsunfall verursacht habe. Zur Abwendung einer angeblich drohenden Haft müsse sie eine Kaution in Höhe von 50.000 Euro zahlen. Im Verlauf der Gespräche meldeten sich angebliche Polizeibeamte, Staatsanwälte, Bankangestellte und Versicherungsmitarbeiter. Selbst Rückrufe der Geschädigten - auch über die angebliche „110“ - führten zurück zu den Tätern, die mit professioneller Gesprächsführung den Eindruck einer echten Amtshandlung vermittelten.

Die zunächst angekündigte Einzahlung beim Amtsgericht wurde schließlich in eine persönliche Geldübergabe geändert. Als eine unbekannte Person an der Wohnanschrift der Geschädigten erschien, verweigerte diese geistesgegenwärtig die Übergabe und zog einen Zeugen hinzu. Daraufhin flüchtete der Geldabholer zu Fuß.

Beispiel 7: Kaiserslautern
Hacker kapern Banking-Programm. Weil er Opfer von Betrügern wurde, hat sich ein Mann aus dem Stadtgebiet am Mittwoch bei der Polizei gemeldet.
Wie der 49-Jährige zu Protokoll gab, wurde sein Computer offenbar „gehackt“. Auf noch nicht geklärte Weise verschafften sich die Unbekannten auch Zugriff auf das Banking-Programm des Mannes, das dieser für seine Tätigkeit für ein Finanzdienstleistungsunternehmen nutzt. Hier gelang es den Tätern, einen insgesamt fünfstelligen Betrag an verschiedene Empfänger im Ausland zu überweisen, bevor der 49-Jährige den Betrug bemerkte. Die Kripo hat die Ermittlungen aufgenommen und versucht, die digitalen Spuren zu verfolgen.

Beispiel 8: Gifhorn (NI)
Aber nicht nur durch Anrufe und E-Mails, sondern auch beim Einkauf im Internet werden die Nutzer angegriffen. Weil diese Angriffe zum Weihnachtsfest zu-

nehmen, warnt die Polizei vor Fake-Shops. Die Familie sitzt bei Duft von Zimt und Tannenzweigen im Wohnzimmer, doch unter dem Baum herrscht gähnende Leere: Das neue Smartphone für die Tochter, schon Wochen zuvor bestellt, ist nie angekommen. Die Bestellbestätigung sah echt aus, der Preis war verlockend günstig - doch der vermeintliche Online-Shop entpuppte sich als Fakeshop. Das Geld ist weg, das Geschenk ebenfalls.

Gerade in der Vorweihnachtszeit, wenn viele Menschen Geschenke bequem im Internet bestellen, nutzen Betrügerinnen und Betrüger die erhöhte Kauflaune gezielt aus. Die Polizei warnt deshalb eindringlich vor Fake-Shops und gibt Tipps, wie man sich schützen kann. Ein klassisches Warnsignal lautet: Wenn ein Angebot zu gut ist, um wahr zu sein, dann ist es das meist auch nicht.

Besonders auffällig sind extrem niedrige Preise für gefragte Produkte wie Smartphones, Spielkonsolen oder Markenkleidung. Oft werden Kundinnen und Kunden dazu verleitet, per Vorkasse zu zahlen - die Ware wird jedoch nie geliefert.

Daneben gibt es eine Reihe weiterer Anzeichen, die auf einen unseriösen Online-Shop hindeuten können. Fehlende oder unvollständige Impressum angaben, unprofessionell gestaltete Webseiten, Rechtschreibfehler oder auffallend schlechte Übersetzungen sollten ebenso misstrauisch machen wie fehlende Kontaktmöglichkeiten oder ausschließlich Vorkasse-Zahlung. Auch übertrieben positive Bewertungen, Gütesiegel ohne Verlinkung oder fragwürdige Domainnamen (etwa mit Tippfehlern oder unbekannten Endungen) können Hinweise auf einen Fakeshop sein.

Die gute Nachricht: Verbraucherinnen und Verbraucher können verdächtige Seiten kostenlos prüfen.

Die Verbraucherzentrale bietet mit dem sogenannten Fakeshop-Finder ein Online-Tool an, mit dem sich Webseiten innerhalb weniger Sekunden bewerten lassen. Wer die Internetadresse eines Shops eingibt, erhält eine Ampelbewertung - Grün bedeutet bisher unauffällig, Gelb steht für Zweifel, und Rot weist auf ein hohes Risiko hin.

Der Fakeshop-Finder ist erreichbar unter www.verbraucherzentrale.de/fakeshopfinder.

Sollten Sie dennoch Opfer eines Fakeshops geworden sein, gilt: Schnelles Handeln. Versuchen Sie umgehend, eine bereits getätigte Zahlung zu stoppen oder rückgängig zu machen. Kontaktieren Sie Ihre Bank, Kreditkartenanbieter oder den Zahlungsdienstleister. Sichern Sie außerdem alle Belege wie E-Mails, Bestellbestätigungen und Screenshots der Webseite und erstatten Sie Anzeige bei der Polizei Als letztes Beispiel ein Betrugsprotokoll eines Betruges unter Einbeziehung Daten einer Online-Bank, einer angeblichen Staatsanwaltschaft und eines angeblichen Rechtanwaltbüros.

Beispiel 9: Gifhorn (NI)
Vermerk eines Betrugsvorganges
1. Am Montag, 08.09.25, teilte die IngDiba-Servicehotline telefonisch mit, dass eine Lastschrift aus dem Ausland vorliege. Da eine Auslandslastschrift für das angegebene Konto ungewöhnlich sei, habe man die Lastschrift blockiert und mit dem Inhaber des Kontos Kontakt aufgenommen. Der Kontoinhaber erklärte, dass eine Lastschriftforderung nicht vorliege. Der Sachbearbeiter von der „IngDiba“ wollte den Sachverhalt mit der IT-Abteilung klären und sich wieder melden.

2. Am Dienstag, 09.09.25, meldete sich der „IngDiba-Sachbearbeiter“ und teilte mit, dass er auf Grund des derzeit hohen Arbeitsaufkommens von der IT-Abteilung noch keine Info erhalten habe, er würde sich jedoch umgehend melden, wenn neue Erkenntnisse vorliegen.

3. Am Donnerstag, 11.09.25, meldete sich der „IngDiba-Sachbearbeiter“ per Telefon erneut und teilte mit, dass er eine Rechtsanwältin der Staatsanwaltschaft Berlin, Rechtsanwältin xxxx, kontaktiert habe und die Angelegenheit bearbeiten werde.

4. Daraufhin meldete sich der Kontoinhaber bei der IngDiba unter der Hotline-Servicenummer 069 342224, die in der IngDiba-App angegeben ist, und fragte nach, welche Begründung für die Kontosperrung vorliegen würde. Der Sachbearbeiter erklärte, er dürfe dieses nicht sagen. Daraufhin wurde er vom Kontoinhaber gebeten, eine Kopie des Antrages, es sollte eine E-Mail vorliegen, ihm zu übersenden. Der Sachbearbeiter betonte, er dürfe dieses nicht, würde es jedoch mit seinem Vorgesetzen klären. Er betonte wieder, einer Übersendung der E-Mail könne er als Sachbearbeiter jedoch nicht zusagen, da er diese Befugnis nicht habe.

5. Kurze Zeit später meldete sich der Sachbearbeiter telefonisch und teilte mit, er habe als Mitarbeiter der Bank Kontakt mit einer Rechtsanwältin der Staatsanwaltschaft xxxx aufgenommen. Die Rechtsanwaltspraxis werde den Kontoinhaber kontaktieren. Das genannte Anwaltsbüro kontaktierte den Kontoinhaber und bestätigte, der Vorgang lege dort vor und man nehme sich der Sache an. Es wurde auch mitgeteilt, dass es sich um eine Anzeige der Staatsanwaltschaft Ankara in der Türkei handele. Seit 2021 versuchen

diese, den Gewinner eines Gewinnspiels, der einen Gewinn von 36.800 € nicht abgeholt hätte, ausfindig zu machen. Die Staatsanwaltschaft hätte das Geld auf einer türkischen Bank deponiert. Der Kontoinhaber bat erneut darum, ihm eine Unterlage darüber zu übersenden. Die RAin lehnte dieses ab, da das Verfahren eröffnet und die Kontosperrung bereits beantragt sei. Es wurde darüber eine Vorgangsnummer der Staatsanwaltschaft in xxxx genannt. Die RAin wies weiter daraufhin, dass ein Antrag für eine Kontosperrung von der Staatsanwaltschaft Ankara/Türkei sowie der deutschen Steuerbehörde in Höhe von 12.300 € vorlege und gleichzeitig eine Strafanzeige bei der Staatsanwaltschaft Berlin gestellt sei. Der Straftatbestand sei eine Steuerhinterziehung, sprich Hinterziehung der Gewinnsteuer.
Ferner bot die RAin an, das Verfahren außergerichtlich abzuwickeln, um hohe Kosten in der Türkei zu sparen. Nach Abschluss des Vorganges würden dem Kontoinhaber alle Unterlagen zugestellt. Damit wäre auch der Strafbestand der Steuerhinterziehung und Geldwäsche sowie Schwarzgeld ausgeschlossen. Es sollten jedoch keine weiteren Behörden eingebunden werden, da dieses eine Störung der Gespräche mit der Türkei erschweren würde. Die Kontakte von deutschen und türkischen Staatsanwaltschaften seinen wesentlich unkomplizierter. Bei diesem Verfahren müsse man jedoch viel Vertrauen zu den Behörden haben. Sie versprach auch, dass sie sich bei ihrem Vorgesetzten informieren würde, die Kontosperrung bei der IngDiba durchzusetzen und sich wieder zu melden.

6. Der Kontoinhaber wurde immer mehr verunsichert und versuchte über das Internet die RAin zu überprüfen. Auf der Internetseite der Staatsanwaltschaft xxxx fand er die Anwaltskanzlei als Partner der Staatsanwaltschaft. Ein Anruf über die IngDiba-App beim Servicecenter der IngDiba bestätigte der gleiche Sachbearbeiter, dass die RAin real wäre und die Kontosperrung nach Rücksprache mit der RAin aufgehoben sei.

7. Nur kurze Zeit später meldete sich erneut die RAin, dass das Verfahren außergerichtlich geklärt wäre. Damit würde ein Steuerverfahren in Deutschland und eine Strafverfolgung beendet werden können. Ferner brauchte kein teurer Anwalt in der Türkei beauftragt werden. Auf Nachfrage, wer ihre Kosten übernehmen würde, teilte sie mit, diese würde die Staatsanwaltschaft xxxx übernehmen. Sie brauche jedoch dafür eine telefonische Bevollmächtigung. Diese Vollmacht wurde vom Kontoinhaber telefonisch erteilt.

8. Gegen 15:00 h meldete sich die RAin erneut und teilte mit, dass die türkische Staatsanwaltschaft sich bereiterklärt hätte, einem außergerichtlichen Verfahren zuzustimmen. Es müsse jedoch vorab eine Zins- und Bearbeitungsgebühr in Höhe von 3.000 € umgehend geleistet werden. Das Geld müsse bis zum 12.09.25 in der Türkei zur Verfügung stehen und über MoneyGram in bar abgewickelt werden. Dieses sollte über eine Mittelsfrau der türkischen Staatsanwaltschaft Frau xxxx xxxxx laufen.

9. Noch am gleichen Tag wurde vom Kontoinhaber das Geld bei dem MoneyGram-Partner eingezahlt und anschließend der RAin die Referenznummern auf den Einzahlungsquittungen mitgeteilt.

11. Am Freitag, 12.09.25, teilte die RAin mit, dass das Geld eingegangen sei und bereits angewiesen.

12. Am Montag, 15.09.25, gegen 15:30 h rief die RAin in Deutschland erneut an und teilte mit, dass die Staatsanwaltschaft Ankara jetzt 7.300 € Gewinnsteuern vorab einfordere. Sie würde dem Kontoinhaber raten, dieses Geld ebenfalls über MoneyGram zu zahlen. Durch diese Zahlung könnte die Steuerabgabe in Deutschland entfallen.

13. Nun wurde der Kontoinhaber misstrauisch und entschloss sich, Hilfe bei der Polizei zu holen sowie eine Anzeige zu stellen. Die Polizei gab Tipps und Ratschläge für das weitere Vorgehen.

14. Noch am Abend wurde vorsichtshalber das Konto vom Kontoinhaber geräumt und die benutzte Servicenummer der IngDiba gesperrt.

15. Am Dienstag, 16.09.25, wurden keine Anrufe mehr angenommen und die IngDiba unter einer anderen Servicenummer kontaktiert und um eine intensive Kontobeobachtung gebeten. Ferner sollte Kenntnis gegeben werden, dass eine Anzeige unter dem Vorgang 2025 011 05448 wegen Betrug gestellt wurde.

16. Auf Anraten der Polizei wurde die Bank unter einer neuen Servicenummer kontaktiert. Der Polizeibeamte wies darauf hin, dass die Bank weder durch Rückrufe oder E-Mail-Kontakte mit den Kunden Kontakt aufnehmen würde.

17. Am 12.12.25 erfolgte die Mitteilung der bearbeitenden hiesigen Staatsanwaltschaft, dass das Strafverfahren gegen die „Geldabholerin“, die in der Türkei nur einen Kurierdienst wahrgenommen habe, eingestellt wurde, da ein zielführender Ermittungserfolg nicht gegeben sei. Eine Beschwerde gegen die Verfahrenseinstellung wäre möglich.

Im Rahmen der Recherche konnte weiter ermittelt werden, dass es die dem Kontoinhaber angegebene Vorgangsnummer bei der Staatsanwaltschaft nicht gab. Bei dem Rechtsanwaltsbüro hatte von Unbe-

kannten ein Identitätsdiebstahl stattgefunden.

Genehmigung für die Veröffentlichung des Vorganges liegt vor.

Vorsicht vor Betrügern

Aktuell kommt es in **Ludwigshafen-Ruchheim** vermehrt zu betrügerischen Anrufen, bei denen unbekannte Personen z. B. Notlagen von angeblichen Angehörigen vortäuschen (sogenannte Schockanrufe), falsche Gewinnversprechen abgeben oder sich fälschlicherweise als Amtsträger wie Staatsanwälte oder Polizeibeamte ausgeben. Mit geschickter Gesprächsführung verunsichern und manipulieren sie ihre Opfer derart, dass sie teilweise sehr hohe Geldbeträge und Wertgegenstände an die Täter überweisen oder sogar persönlich übergeben.

Die Polizei nimmt das zum Anlass, um Präventionshinweise zu geben. So schützen Sie sich vor Schockanrufen: - Legen Sie sofort auf, wenn angebliche Polizisten, Staatsanwälte oder Angehörige Sie telefonisch unter Druck setzen oder Geld fordern.

- Rufen Sie selbstständig die echte Polizei unter 110 an - nutzen Sie dazu eine neue Verbindung und nicht die Rückruffunktion auf dem Display.

Polizei warnt vor Smishing - Betrug per SMS nimmt zu

Die Polizei warnt aktuell vor sogenannten Smishing-Angriffen. Dabei handelt es sich um Betrugsversuche, die über SMS, Messenger-Dienste oder ähnliche Textnachrichten erfolgen. Kriminelle geben sich in diesen Nachrichten häufig als Banken, Paketdienste, Behörden oder andere vertrauenswürdige Institutionen aus und versuchen, die Empfängerinnen und Empfänger zur Preisgabe sensibler Daten zu bewegen. Typischerweise enthalten die Nachrichten einen dringenden Handlungsaufruf, etwa wegen angeblich gesperrter Konten, nicht zugestellter Pakete oder offener Rechnungen. In vielen Fällen sind Links enthalten, die auf täuschend echt gestaltete Internetseiten führen. Dort werden Login-Daten, Passwörter oder Bankinformationen abgefragt oder es wird Schadsoftware installiert. Die Polizei weist darauf hin, dass Smishing besonders erfolgreich ist, da SMS häufig schneller gelesen werden als E-Mails und viele Menschen es gewohnt sind, wichtige Informationen - etwa Sicherheitscodes oder Lieferbenachrichtigungen - per Kurznachricht zu erhalten. Auch bekannte oder scheinbar vertrauenswürdige Absendernummern bieten keinen verlässlichen Schutz, da Kriminelle Rufnummern manipulieren können (sogenanntes SMS-Spoofing). So erkennen Sie verdächtige Nachrichten: - unbekannte oder ungewöhnliche Absender - Rechtschreib- oder Grammatikfehler - starker Zeitdruck oder Drohungen („Handeln Sie sofort“) - Inhalte, die nicht zur eigenen Situation passen - enthaltene Links zu angeblichen Logins oder Bestätigungen Die Polizei empfiehlt, keine Links aus verdächtigen Nachrichten anzuklicken und keine persönlichen oder finanziellen Daten preiszugeben. Im Zweifel sollten Betroffene die angeblich kontaktierende Institution über die offiziell bekannten Kontaktwege selbst kontaktieren. Falls Sie bereits auf eine solche Nachricht reagiert haben: - Trennen Sie Ihr Smartphone umgehend vom Internet. - Lassen Sie das Gerät auf Schadsoftware überprüfen. - Ändern Sie betroffene Passwörter. - Kontaktieren Sie Ihre Bank, falls Bankdaten betroffen sein könnten. - Erstatten Sie Anzeige bei der Polizei. Verdächtige Nachrichten können zudem bei der Bundesnetzagentur sowie beim jeweiligen Mobilfunkanbieter gemeldet werden. Die Polizei rät, wachsam zu bleiben und insbesondere in der Voweihnachtszeit erhöhte Vorsicht walten zu lassen. Und es kann Jeden treffen. Denn die Täter agieren äußerst geschickt und skrupellos. Dabei passen sie ihre Gesprächstaktiken und Vorgehensweisen ständig an.

Infos: Polizeiinspektion Emsland/Grafschaft Bentheim, Polizeipräsidium Rheinpfalz, Polizeidirektion Ludwigshafen, Polizeiinspektion Schifferstadt, Polizeipräsidium Westpfalz, Polizeipräsidium Westpfalz, Polizeiinspektion Verden / Osterholz, Polizeiinspektion Wilhelmshaven/Friesland, Polizeiinspektion Gifhorn

Der Europäische Rechnungshof hat nun einen Sonderbericht über die Betrugsbekämpfungsarchitektur vorgelegt. In dem Bericht werden die für die Betrugsbekämpfung zuständigen Stellen der EU – die Europäische Staatsanwaltschaft (EUStA), das Europäische Amt für Betrugsbekämpfung (OLAF), die Agentur der Europäischen Union für justizielle Zusammenarbeit in Strafsachen (Eurojust) und die Agentur der Europäischen Union für die Zusammenarbeit auf dem Gebiet der Strafverfolgung (Europol) – unter die Lupe genommen.

Zusammenfassend stellten die Prüfer fest, dass es Schwachstellen beim Kampf der EU gegen Betrug gibt. Dem Bericht des Europäischen Rechnungshofs zufolge wird die Betrugsbekämpfung der EU durch Mängel beim Informationsaustausch zwischen den wichtigsten dafür zuständigen Stellen beeinträchtigt. Dies habe Auswirkungen auf die Zahl der Untersuchungen und führe zu Verzögerungen. Außerdem könne die EU-Kommission ihrer Kontrollfunktion und allgemeinen Zuständigkeit für den Schutz des EU-Haushalts nicht umfassend nachkommen. Zwar würden infolge der Untersuchungen des Europäischen Amts für Betrugsbekämpfung (OLAF) und der Europäischen Staatsanwaltschaft (EUStA) Millionenbeträge veruntreuten Geldes eingezogen, der EU-Kommission sei jedoch nicht bekannt, ob auch alle dem EU-Haushalt geschuldeten Beträge zurückgezahlt würden. Vor dem Hintergrund der laufenden Überprüfung der Betrugsbekämpfung in der EU fordern die Prüfer ein neues System, um die Prüfung

von Verdachtsfällen und die Durchführung von Untersuchungen zu vereinfachen.

Im Rahmen der Betrugsbekämpfung der EU ermittelt die Europäische Staatsanwaltschaft bei mutmaßlichem Betrug, das Europäische Amt für Betrugsbekämpfung hingegen ist für Verwaltungsuntersuchungen zuständig. Das OLAF und die EUStA werden außerdem von der Agentur der Europäischen Union für justizielle Zusammenarbeit in Strafsachen (Eurojust), der Agentur der Europäischen Union für die Zusammenarbeit auf dem Gebiet der Strafverfolgung (Europol) und den nationalen Behörden unterstützt.

„Eine wirksame Zusammenarbeit zwischen allen an der Betrugsbekämpfung beteiligten Stellen – von den EU-Ermittlungsbehörden bis hin zu den nationalen Polizei- und Justizbehörden – ist von entscheidender Bedeutung, um Betrüger in Schach zu halten“, so Katarína Kaszasová, das für die Prüfung zuständige Mitglied des Rechnungshofs. „Die laufende Überprüfung der Betrugsbekämpfungsarchitektur der EU ist die ideale Gelegenheit, um Mängel des Systems in puncto Informationsaustausch und Überwachung zu beheben.“

Die Prüfer stellten fest, dass der rechtliche Auftrag des OLAF, der EUStA, von Eurojust und Europol klar definiert ist. Die von ihnen unabhängig wahrgenommenen Aufgaben ergänzten einander und könnten somit einen wirksamen Schutz vor Betrug bieten. Die Stellen schätzten die gegenseitige Unterstützung, die bei Bedarf beantragt werden könne, hätten von dieser Möglichkeit aber in den letzten Jahren nur in relativ wenigen Fällen Gebrauch gemacht.

Die Verfahren für den Umgang mit mutmaßlichem Betrug, welcher der EU finanziell schade, seien komplex. So führten die unterschiedlichen Vorschriften für die Meldung von Verdachtsfällen dazu, dass dieselben Fälle sowohl dem OLAF als auch der EUStA gemeldet würden, was den Verwaltungsaufwand erhöhe. Darüber hinaus stelle das System nicht sicher, dass alle Meldungen, bei denen überprüft werden sollte, ob eine kriminelle Handlung vorliegt, bei der EUStA eingehen. Die Verfahren für eine Weiterleitung von Fällen vom OLAF an die EUStA seien umständlich, und der Austausch von Informationen der EUStA mit dem OLAF sei begrenzt, was den Spielraum für zusätzliche Schutzmaßnahmen schmälere.
Zwischen 2022 und 2024 seien dem OLAF und der EUStA insgesamt 27 000 Betrugsverdachtsmeldungen zugegangen. Bei einem Drittel sei eine Untersuchung eingeleitet worden. Aus den vorliegenden Zahlen gehe hervor, dass die EU-Einrichtungen dem OLAF dreimal mehr Betrugsvorwürfe gemeldet hätten als der EUStA und bei vielen Mitgliedstaaten eine große Diskrepanz bestehe zwischen der Höhe der verwalteten EU-Mittel und der Anzahl der von ihnen übermittelten Verdachtsmeldungen. Die Prüfer fordern die EU-Kommission auf, die Gründe für diese Diskrepanzen zu analysieren und den Ursachen für auffällig niedrige Meldequoten nachzugehen.
Im Anschluss an seine Untersuchungen für den genannten Zeitraum habe das OLAF empfohlen, dass Mittel in Höhe von 615 Millionen Euro an den EU-Haushalt zurückerstattet werden sollten. Bis Ende 2024 seien bereits 23 Millionen Euro zurückgezahlt worden. Im selben Zeitraum habe die EUStA Vermögenswerte in Höhe von 3 Milliarden Euro eingefroren. Infolge der Ermittlungen der EUStA hätten die Gerichte im Jahr 2024 die nationalen Behörden angewiesen, illegal erworbene Mittel in Höhe von 232 Millionen Euro von den Betroffenen einzuziehen. Die EU-Kommission verfüge jedoch über keinen Mechanismus, um zu überwachen, ob die von den Gerichten angeordneten Einziehungen erfolgt seien und der gesamte geschuldete Betrag auch tatsächlich an den EU-Haushalt zurückgezahlt worden sei. Daher müsse die EU-Kommission die Ergebnisse der Betrugsermittlungen besser nachverfolgen, betonen die Prüfer.

Hintergrund

Die Betrugsbekämpfungsarchitektur der EU sieht zwei Möglichkeiten zur Untersuchung potenzieller Betrugsfälle vor: vom OLAF durchgeführte Verwaltungsuntersuchungen und von der EUStA durchgeführte strafrechtliche Ermittlungen. Die beiden Stellen können bei der justiziellen Zusammenarbeit von Eurojust und bei der polizeilichen Zusammenarbeit von Europol unterstützt werden. Die Prüfer untersuchten, ob die Mandate der EUStA, des OLAF, von Eurojust und Europol klar definiert sind, was ihre Zuständigkeiten bei der Betrugsbekämpfung und die gegenseitige Unterstützung betrifft. Sie prüften außerdem den Informationsaustausch zwischen der EUStA und dem OLAF, die Aufsicht durch die Europäische Kommission sowie deren allgemeinere Rolle bei der Sicherstellung des Schutzes der finanziellen Interessen der EU.

Text: Pressestelle der Europäischen Staatsanwaltschaft