LUG & TRUG

Wirtschaft Spezial

Wissen und Information zum Schutz vor Betrug

GRAZ

GEMEINSAM.SICHER IN GRAZ

POLIZEI

Liebe Leserinnen und Leser!

Dass sich das Betrugsgeschehen zunehmend ins Internet verlagert, ist hinlänglich bekannt. Dass sich Betrüger dabei vermehrt auf Klein- und Mittelunternehmen konzentrieren, ist hingegen ein Phänomen, das sich bei uns in Graz eher sprunghaft entwickelt hat. Die Täter wissen zu gut: In KMUs gibt es eher Sicherheitslücken als in Großkonzernen, die hohe Summen in Sicherheitstechnik und Mitarbeiterschulungen investieren können und dies auch tun.
Wir möchten, dass auch kleinere Unternehmen vor Betrug besser geschützt sind. Speziell Ihnen, den Wirtschaftstreibenden in Klein- und Mittelunternehmen, und Ihren MitarbeiterInnen ist daher diese Ausgabe von „Lug & Trug" gewidmet. Auf den folgenden Seiten erfahren Sie anhand praktischer Beispiele, wie Betrüger, die sich auf KMUs spezialisiert haben, häufig vorgehen, wie Sie Ihr Unternehmen gemeinsam mit Ihren MitarbeiterInnen schützen können und wie man im Schadensfall am besten agiert.
Wie immer gilt, und das ist unser Appell an Sie: Sollte Ihr Unternehmen geschädigt worden sein oder der Verdacht bestehen, dass jemand versucht, es zu schädigen, dann verständigen Sie bitte umgehend die Polizei über den Notruf 133! Nur so können die ErmittlerInnen schnellstmöglich tätig werden und Sie – und auch andere – vor weiterem Schaden bewahren.

Ihr
GEMEINSAM.SICHER-Team

Gemeinsam für mehr Sicherheit – von links: Werner Miedl (GEMEINSAM.SICHER), Klaus Murtinger (Kriminalreferat der Grazer Polizei, Betrugsgruppe), Manuel Leitner (Sicherheitskoordinator für Graz), Stadtpolizeikommandant Kurt Kemeter, Linda Trinkl (GEMEINSAM.SICHER), Daniela Schuster (Kriminalreferat, Betrugsgruppe), Dr. Klaus Gstirner (Obmann Verein GEMEINSAM.SICHER in Graz)

Foto: GEMEINSAM.SICHER in Graz

Inhalt

Vorworte 4
Betrug erkennen 6
CEO-Betrug 8
Man in the Middle 10
Kontodatendiebstahl (Pishing) 12
DDoS-Attacke 14
Erpressungstrojaner 16
Falschgeld 17
Kreditkartenbetrug 18
Scheckbetrug 20
Identitätsbetrug 22
Inkassobetrug 24
Weitere Betrugsformen 25
Adressen & nützliche Links 26

1. Auflage, November 2017

Zur leichteren Lesbarkeit wurde zum Teil auf eine geschlechtsneutrale Schreibweise verzichtet, womit keine Aussage über die tatsächliche Geschlechterverteilung von StraftäterInnen getroffen wird.
Die aktuelle österreichische Gerichtsstatistik weist 85,4 Prozent aller Verurteilten als männlich aus (Quelle: Gerichtliche Kriminalstatistik 2016, Statistik Austria).

Impressum
Verein GEMEINSAM.SICHER in Graz, c/o Sicherheitsinformationszentrum Graz, Keplerstraße 25, 8020 Graz; ZVR: 066269364 • Redaktion: Klaus Murtinger, Daniela Schuster, Linda Trinkl
Layout und Gestaltung: netWERKER Mediahaus OG, 8551 Wies; www.netwerker.at
Druck: Druck.at • Für den Inhalt verantwortlich: Werner Miedl

Mit der zunehmenden Vernetzung unseres Alltags wird auch die Frage nach der Online-Sicherheit immer wichtiger. Internetkriminalität, darunter auch der Betrug im Netz, ist leider ein expandierender Teil der Kriminalitätsfälle geworden. Aber unsere Ermittlungsbehörden stellen sich in vorbildlicher Weise diesen sich ständig erneuernden Herausforderungen der Kriminalitätsbekämpfung im Netz.

Ich darf Sie bitten, die Sicherheitstipps in dieser Broschüre zu beherzigen und Ihnen versichern, dass die Polizei in allen Fragen Ihrer persönlichen Netz-Sicherheit der ideale Ansprechpartner für Sie oder Ihr Unternehmen ist.

Ihr
Mag. (FH) Mario Eustacchio
Vizebürgermeister der Stadt Graz

Foto: Pachernegg

Die Digitalisierung hat uns zweifelsohne in ein neues Zeitalter geführt: Noch nie war es so einfach, Arbeitsabläufe zu planen, zu steuern und durchzuführen. Mit den Erleichterungen, die uns Computer und Technik bieten, sind allerdings auch die Herausforderungen und Risiken in puncto Sicherheit gestiegen: Neben klassischen Betrugsformen am Telefon oder im persönlichen Umgang miteinander werden heutzutage Datenbanken gehackt, E-Mails gefälscht und Internetauftritte manipuliert. Die Täter agieren weit über den Staatsgrenzen hinweg und sind, wenn überhaupt, nur schwer dingfest zu machen.
Für Wirtschaftstreibende ist es daher umso wichtiger, auf Unternehmenssicherheit zu achten. Mein Appell: Investieren Sie in Sicherheitssoftware, schulen und sensibilisieren Sie Ihre Mitarbeiterinnen und Mitarbeiter und nutzen Sie die Informationsangebote der Polizei und GEMEINSAM.SICHER – zum Beispiel die Cyber-Security-Beratung in unserem Sicherheitsinformationszentrum (SINFO), die in Kooperation mit der TU Graz angeboten wird. Arbeiten wir gemeinsam daran, dass sich Graz als Wirtschaftsstandort weiterhin lohnt – aber nicht für Kriminelle, sondern für Sie als Unternehmer und Ihre MitarbeiterInnen.

Ihr
Mag. Siegfried Nagl
Bürgermeister der Stadt Graz

Foto: Fischer

Betrug erkennen

Wie im Privatleben, so gilt auch im Berufsalltag: Wer über die Tricks und Methoden von Betrügern Bescheid weiß und entsprechend vorsichtig agiert, kann sich besser schützen.

Foto: fotolia.de

Wirtschaftsbetriebe, und hier vor allem Klein- und Mittelunternehmen, werden für Betrüger zunehmend attraktiver. Das haben auch unsere Erfahrungen in Graz gezeigt: In den vergangenen Monaten und Jahren ist die Zahl entsprechender Betrugsfälle auch bei uns gestiegen.

Um die Methoden der Täter (be-)greifbarer zu machen, stellen wir Ihnen auf den folgenden Seiten Fälle vor, mit denen wir in dieser oder ähnlicher Form bereits konfrontiert waren. Da Betrüger allerdings erfinderisch sind und immer wieder neue Vorgangsweisen entwickeln, raten wir Ihnen grundsätzlich:

- Bleiben Sie auf dem Laufenden und informieren Sie sich aktiv! Wenn Sie zum Beispiel über soziale Medien oder aus Zeitungen von einer neuen CEO-Betrugswelle erfahren, können Sie Ihre Mitarbeiterinnen und Mitarbeiter entsprechend sensibilisieren.

- Setzen Sie auf Kommunikation! Sorgen Sie dafür, dass der Informationsfluss in Hinblick auf Betrugswarnungen innerhalb Ihres Unternehmens funktioniert.

- Geben Sie Handlungssicherheit! Legen Sie klare Regeln fest, damit Ihre MitarbeiterInnen wissen, wie sie bei Verdachtsfällen richtig agieren.

- Setzen Sie auf Weiterbildung! Nutzen Sie zum Beispiel die Schulungsangebote der Österreichischen Nationalbank oder der Kriminalprävention – Sie investieren damit auch in die Sicherheit Ihres Unternehmens.

Für mehr Sicherheit vor Betrug abseits des Berufslebens möchten wir Ihnen und Ihren MitarbeiterInnen unsere „Lug & Trug"-Ausgaben „Täuschung durch Technik" und „Betrugsformen im Alltag" ans Herz legen. Diese sind unter anderem im Sicherheitsinformationszentrum, im Grazer Rathaus oder als kostenloser Download auf www.gemeinsamsichergraz.at erhältlich.

Klaus Murtinger
Chefinspektor, Leiter der Betrugsgruppe im Stadtpolizeikommando Graz

Daniela Schuster
Abteilungsinspektorin, stellvertretende Leiterin der Betrugsgruppe im Stadtpolizeikommando Graz

Foto: GEMEINSAM.SICHER in Graz

CEO-Betrug

Auch CEO Fraud, Fake-President-Trick oder Cheftrick genannt: Ein „falscher" Chef gibt eine Überweisung in Auftrag, um sich an Firmengeldern zu bereichern.

Was ist passiert?

Bei der Kontrolle der Geschäftskontoauszüge stelle ich fest, dass gestern 57.890 Euro durch Spationieren auf das Konto eines mir unbekannten Geschäftspartners überwiesen wurden. Ich kontaktiere den verantwortlichen Prokuristen, um Information über das Geschäft einzuholen. Der Prokurist ist ganz verwundert und gibt mir zu verstehen, dass ich selbst es war, der ihm diesen Auftrag gegeben hat. Er zeigt mir mehrere E-Mails, in denen er mehrfach auf die besondere Dringlichkeit und Vertraulichkeit des Geschäftes hingewiesen wurde. Es sieht tatsächlich so aus, als ob die Nachrichten von mir stammen, aber das kann nicht sein! Wir versuchen sofort, die Transaktion zu stoppen, aber laut Auskunft des Bankangestellten ist das Geld bereits am Empfängerkonto eingelangt und könnte bereits behoben worden sein.

Was liegt vor?

Beim CEO-Betrug geben sich Täter, nachdem sie Informationen jeglicher Art über das von ihnen ausgewählte Unternehmen gesammelt haben, zum Beispiel als Geschäftsführer (CEO) des Unternehmens aus und veranlassen bei einem Unternehmensmitarbeiter den Transfer eines größeren Geldbetrages ins Ausland. Um den Mitarbeiter zu täuschen, nutzen die Täter Informationen, die Unternehmen in Wirtschaftsberichten, im Handelsregister, auf ihrer Webseite oder in Werbebroschüren veröffentlichen. In anderen Fällen schleusen sie Spionagesoftware in das Firmennetzwerk ein und gelangen so an Informationen über die Geschäftsleitung, Buchhaltung und Geschäftsbeziehungen. Die Empfängerkonten beim CEO-Betrug befinden sich zumeist im Ausland, was es den Tätern leicht macht, anonym zu bleiben.

Die Polizei empfiehlt:

- Achten Sie darauf, welche Informationen über Ihr Unternehmen öffentlich sind bzw. wo und was Sie und Ihre MitarbeiterInnen im Zusammenhang mit Ihrem Unternehmen publizieren!
- Führen Sie klare Abwesenheitsregelungen und interne Kontrollmechanismen ein!
- Sensibilisieren Sie Ihre MitarbeiterInnen in Bezug auf diese Betrugsart!
- Bei ungewöhnlichen Zahlungsanweisungen sollten vor Veranlassung der Zahlung folgende Schritte durchgeführt werden:
  1. Überprüfen der E-Mails auf Absender adresse und korrekte Schreibweis
  2. Verifizieren der Zahlungsaufforderung über Rückruf bzw. schriftliche Rückfrage beim genannten Auftraggeber
  3. Kontaktaufnahme mit der Geschäftsleitung bzw. dem Vorgesetzten
- Versuchen Sie im Schadensfall die Geldtransaktion so rasch wie möglich über Ihre Bank zu stoppen und informieren Sie die Polizei. Sichern Sie in jedem Fall den E-Mail-Verkehr und stellen Sie auch die Transaktionsbelege für die Ermittlungen zur Verfügung.

Foto: fotolia.de

Man in the Middle

Das Vortäuschen einer Kontodatenänderung, um Firmengelder auf das Konto der Täter umzuleiten.

Was ist passiert?

Wir urgieren zum dritten Mal die Lieferung der bestellten und bereits bezahlten Ware bei unserem ausländischen Geschäftspartner. Diesmal lege ich dem Schriftverkehr auch die Zahlungsbestätigung bei, doch der Lieferant beharrt darauf, dass bei ihm keine Zahlung eingegangen ist.
Wo sind unsere 125.780 Euro geblieben? Im Zuge interner Besprechungen stellt sich heraus, dass eine Mitarbeiterin in der Buchhaltung ein Schreiben des Lieferanten über dessen Kontodatenänderung erhalten hat. Sie hat die Daten entsprechend geändert und die Überweisung des offenen Betrages auf das neue Geschäftskonto des Lieferanten veranlasst. Der Lieferant teilt mit, dass dieses Schreiben nicht von ihm stammt und dass er keine neue Kontoverbindung hat.
Ich weiß nicht, wie ich den Betrieb weiterführen soll. Unser Geld ist verloren und der Lieferant weigert sich, ohne Vorauszahlung zu liefern.

Was liegt vor?

Bei diesem Angriff täuscht der Täter als „Dritter in der Leitung" zwei Kommunikationspartner, indem er ihnen jeweils die Identität des anderen vorspiegelt. Der in der Mitte sitzende Angreifer entschlüsselt die Daten der beiden Kommunikationspartner und kann so beispielsweise gesicherte SSL-Verbindungen zum Onlinebanking mitlesen und sich in die Kommunikation einschalten. Dies gibt ihm auch die Möglichkeit, einen der Beteiligten durch eine gefälschte Nachricht dazu zu bringen, Geld auf das Konto des Täters zu überweisen.

Die Polizei empfiehlt:

- Achten Sie darauf, dass Sie nur sichere Verbindungen – also https- und keine http-Verbindungen – nutzen.
- Hinterfragen Sie die Kontoänderungen bei Ihren Geschäftspartnern. Verwenden Sie dazu bereits bekannte Telefonnummern bzw. E-Mail-Adressen und vermeiden Sie den neu angebotenen Kontakt.
- Überprüfen Sie ganz genau, ob ein SSL-Zertifikat nicht schon abgelaufen ist und ob es von einer vertrauenswürdigen Zertifizierungsstelle ausgestellt wurde.
- Meiden Sie frei zugängliche VPN-Netze und Proxy-Server.
- Ändern Sie in regelmäßigen Abständen Ihre Passwörter und verwenden Sie die bereits genutzen nie wieder.
- Wählen Sie sich nicht in öffentliche Netze ein und seien Sie auch beim WLAN im Hotel misstrauisch. Vermeiden Sie es unbedingt, irgendetwas zu installieren oder herunterzuladen, wenn Sie über ein solches Netz mit dem Internet verbunden sind. Nehmen Sie auch auf keinen Fall Zahlungen vor und melden Sie sich nicht bei Ihren Konten in sozialen Medien oder bei Ihrem E-Mail-Provider an.

Foto: fotolia.de

Kontodatendiebstahl (Phishing)

Die Täuschung von Bankkunden zur Bekanntgabe von Bankdaten oder die unbemerkte Installation von Computerprogrammen, um unberechtigt Geld vom Konto zu beheben.

Was ist passiert?

In der Buchhaltung langt eine E-Mail von unserer Bank ein, in der wir aufgefordert werden, ein Sicherheitsupdate durchzuführen. Ich werde über einen Link zu einem Formular weitergeleitet und gebe dort alle erforderlichen Daten ein.
Am nächsten Tag fordert mich der Chef auf, die Überweisung von 46.660 Euro zu erklären, die ich angeblich tags zuvor veranlasst habe. Es sieht so aus, als ob ich eine Online-Transaktion mit den erforderlichen Codes freigegeben hätte.
Bei der Bank wird uns gesagt, dass sie uns niemals zu einem Sicherheitsupdate oder zur Eingabe von Daten aufgefordert hätten. Zum Glück kann die Transaktion bei der Bank gerade noch gestoppt werden, sonst wäre ich meinen Job jetzt wohl los.

Was liegt vor?

Betrüger versuchen ihre Opfer mit E-Mails auf gefälschte Bankseiten zu locken, wo der Kunde zur angeblichen Verbesserung der Datensicherheit zur Eingabe und Bestätigung seiner Bankdaten aufgefordert wird. Tatsächlich können die Betrüger mit diesen Daten Geld vom Konto des Kunden überweisen.
In anderen Fällen verschicken die Betrüger E-Mails an Bankkunden, die versteckte Computerprogramme zur Ausspähung von Informationen enthalten. So gelangen die Täter unbemerkt vom Kunden an dessen Bankdaten und können Überweisungen veranlassen. Zusätzlich kann das Handy durch Anbieten von Gratis-Apps mit Schadprogrammen infiziert werden. Dadurch gelangen die Betrüger auch an Bankdaten (TAN-Code), die an das Handy geschickt werden.

Die Polizei empfiehlt:

- Öffnen Sie Webseiten von Banken immer nur durch Eingabe der offiziellen Adresse.
- Folgen Sie keinen Links, die Sie per E-Mail erhalten.
- Bedenken Sie: Keine Bank fordert Sie zur Eingabe von Bankdaten auf, die Bank kennt Ihre Daten!
- Werden Sie misstrauisch, wenn das angebliche Schreiben Ihrer Bank Rechtschreibfehler aufweist oder in unkorrektem Deutsch verfasst ist.
- Verwenden Sie seriöse Virenschutzprogramme auf PC und Handy und halten Sie diese immer aktuell.
- Achten Sie darauf, welche Software Sie auf PC und Handy installieren.
- Kontrollieren Sie regelmäßig Ihren Kontostand.
- Verständigen Sie im Schadensfall sofort Ihre Bank und die Polizei.
- Stellen Sie der Polizei im Schadensfall PC und Handy unverändert zur Datensicherung zur Verfügung.

Foto: fotolia.de

DDoS-Attacke

Die Blockade des Internetauftritts, um die Wettbewerbsfähigkeit der Firma zu beeinträchtigen oder im Hintergrund laufende Betrugshandlungen zu verschleiern.

Was ist passiert?

Ich bin Mitarbeiter eines Versandhauses und erhalte seit Stunden telefonisch Beschwerden von Kunden, die schon den ganzen Tag nicht auf unseren Onlineshop zugreifen können.
Ich verständige unseren Techniker, der mir nach einer Systemüberprüfung mitteilt, dass es offenbar seit rund einem Tag zu einem Totalausfall der Firmenwebsite gekommen ist und er das Problem nicht lösen kann. Wenn wir nicht bald wieder online sind, dürfte der Geschäftsentgang enorm sein. Ich weiß gar nicht, wie ich der Firmenleitung diesen Umsatz- und Imageschaden erklären soll.

Was liegt vor?

Mit „Distributed Denial of Service"-Attacken (DDoS) verfolgen Angreifer das Ziel, Server oder IT-Systeme mit einer großen Anzahl an Anfragen zu bombardieren, bis diese ihren Dienst einstellen und Websites oder andere Internetservices nicht mehr aufrufbar sind.
Hintergrund dieser DDoS-Attacken sind häufig persönliche, politische oder wirtschaftliche Interessen der Angreifer. Deshalb richten sich DDoS-Angriffe in der Regel nicht gegen den Provider, sondern direkt gegen die Website der Seiteninhaber bzw. von Unternehmen, die durch den Angriff beeinträchtigt werden soll. Für eine DDoS-Attacke bedienen sich Kriminelle spezieller Schadsoftware, mit der sie Hunderte ungeschützte Rechner infizieren und so die Kontrolle über diese gewinnen. Mehrere infizierte Rechner bilden dann ein sogenanntes Botnetz, das die Täter nutzen, um massenweise Server zu attackieren. Um eine Website zu boykottieren, senden die gekaperten Rechner Datenpakete an den jeweiligen Webserver, bis dieser keine Kapazitäten mehr hat, um die Daten zu verarbeiten und in der Folge seinen Dienst einstellt.

Die Polizei empfiehlt:

- Wählen Sie sichere Kennwörter für Router, Netzwerke und vernetzte Geräte, damit nicht Unberechtigte die Kontrolle über diese erlangen können.
- Wählen Sie einen Provider, der grundsätzlich Schutz gegen DDos-Angriffe anbietet.
- Führen Sie regelmäßig ein Monitoring der Serverauslastung durch. Messen Sie in einem Stresstest, wie Ihre Infrastruktur auf erhöhte Nachfrage (zum Beispiel im Weihnachtsgeschäft) reagiert.

Foto: fotolia.de

Erpressungstrojaner

Die Verschlüsselung von Computerdateien, um Geld für die Entsperrung zu erpressen.

Was ist passiert?

Ich sitze im Büro und bearbeite gerade eine Onlinebestellung, als plötzlich keine Eingabe mehr möglich ist. Auf dem Bildschirm erscheinen sonderbare Zeichen und ich erhalte die Mitteilung, dass der PC gesperrt ist. Für die Zusendung eines Codes, mit dem der Computer wieder freizuschalten wäre, soll ich drei Bitcoins, also nach aktuellem Kurs etwa 17.000 Euro, an den Erpresser zahlen. Ich bin verzweifelt, all unsere Kundendaten und die gesamte Buchhaltung sind auf dem Rechner gespeichert und unser Unternehmen ist lahmgelegt. Soll ich zahlen?

Was liegt vor?

Erpressungstrojaner – zum Beispiel mit dem Namen CryptoLocker, Locky oder TeslaCrypt – werden von Betrügern als E-Mail-Anhang verschickt und auf dem PC gespeichert oder das Schadprogramm installiert sich während der Internetnutzung unbemerkt selbst. Diese Schadsoftware sperrt den Computer bzw. verschlüsselt die gespeicherten Daten (Fotos, Dokumente, Videos etc.) und lässt sich meist nicht von firmeninternen IT-Verantwortlichen entfernen.
Der Täter verspricht bei Bezahlung des geforderten Geldbetrages die Zusendung eines Entschlüsselungscodes.

Die Polizei empfiehlt:

- Halten Sie Ihr Betriebssystem stets auf dem aktuellen Stand.
- Öffnen Sie keine E-Mails oder Anhänge aus unbekannten Quellen.
- Surfen Sie nicht auf unsicheren Webseiten.
- Sorgen Sie für eine gute Antivirenlösung und halten Sie diese immer auf dem neuesten Stand.
- Sichern Sie Ihre Daten durch regelmäßige Backup-Speicherungen auf externen Datenträgern.
- Leisten Sie keine Zahlungen an den Erpresser und informieren Sie die Polizei!

Foto: fotolia.de

Falschgeld

Die Krux mit dem unwissentlichen Annehmen, dem Besitz und der Weitergabe von gefälschten Banknoten und Münzen.

Was ist passiert?

Ich habe Schlussdienst an der Supermarktkasse. Es ist kurz vor Geschäftsschluss und an meiner Kassa steht immer noch eine lange Warteschlange. Dabei wollte ich gerade heute ins Kino gehen. Ich fertige die Kunden so schnell wie möglich ab.
Erst beim Abrechnen fällt mir auf, dass sich einer der 100-Euro-Scheine ganz eigenartig anfühlt. Ich fürchte, ich habe einen gefälschte Hunderter in meiner Kassa.
Der Chef verlangt, dass ich den Schein zur Polizei bringe und den Schaden bezahle.
Die Polizei überprüft jetzt sogar, ob ich etwas mit der Sache zu tun habe. Das Geld bekomme ich jedenfalls nicht ersetzt.

Was liegt vor?

Betrüger nutzen die mangelnde Aufmerksamkeit und Kenntnis ihrer Opfer, um „Blüten" zur Bezahlung zu verwenden. Das falsche Geld ist dem echten täuschend ähnlich und kann praktisch überall in Umlauf gebracht werden. Am beliebtesten sind das Gedränge an der Supermarktkasse, schummriges Licht von Nachtlokalen, Tankstellen und Taxis.
Wer Falschgeld entgegennimmt, hat den doppelten Schaden: Es gibt keine Entschädigung und man macht sich selbst strafbar, wenn man es weitergibt.

Die Polizei empfiehlt:

- Machen Sie sich – vor allem dann, wenn Sie als MitarbeiterIn oder UnternehmerIn im Handel tätig sind – mit den aktuellen Sicherheitsmerkmalen der Euro-Noten vertraut.
- Sehen Sie sich dazu auch die Tipps auf der Website der Österreichischen Nationalbank an (www.oenb.at/Bargeld/Falschgeld) und nutzen Sie das Schulungs- und Informationsangebot der OeNB.
- Geben Sie im Verdachtsfall kein Falschgeld weiter – damit machen Sie sich strafbar!
- Wenn Sie den Verdacht haben, Falschgeld erhalten zu haben, benachrichtigen Sie bitte sofort die Polizei, um ein rasches Handeln zu ermöglichen.

Foto: fotolia.de

Kreditkartenbetrug

Die Verwendung gestohlener oder gefälschter Kreditkarten bzw. die widerrechtliche Verwendung von Kartendaten.

Was ist passiert?

Ein Kunde betritt das Geschäft und sieht sich in der Abteilung für Elektronik um. Ich biete ihm ein Beratungsgespräch an, aber der Kunde scheint sich bereits entschieden zu haben. Er kommt mit zwei hochwertigen Laptops, drei Smartphones und einigem teuren Zubehör zur Kassa und möchte den riesigen Betrag mit seiner Kreditkarte bezahlen. Zuerst erhalte ich eine Fehlermeldung am Kassenterminal, aber zum Glück hat der Mann eine zweite funktionierende Karte.
Einige Tage später werde ich von der Kriminalpolizei als Zeuge geladen. Scheinbar war der Mann ein Betrüger und hat in mehreren Geschäften mit gefälschten Karten bezahlt.

Was liegt vor?

Betrüger können auf verschiedene Weise an Kreditkarten oder an Kreditkartendaten gelangen. Sie erbeuten zum Beispiel durch Taschen- oder Gelegenheitsdiebstähle Kreditkarten, die sie – oft in organisierten Gruppen – widerrechtlich zur Bezahlung hochwertiger Elektronik, teurer Parfums und Markenkleidung verwenden.
Ebenso können Kreditkarten von einem Betrüger kopiert werden, der als Kassier, Kellner oder Hotelangestellter arbeitet. Mit diesen Daten fertigen Komplizen Duplikate an, die mit falschen Namen versehen werden.
In anderen Fällen gelangen Betrüger auf illegale Weise (beispielsweise durch Hacking) an Kartendaten, die nach Einkäufen im Internet gespeichert bleiben. Diese Datensätze werden von den Betrügern entweder selbst zur Bezahlung von Onlinebestellungen verwendet oder im Internet weiterverkauft.
Bei grober Missachtung der Sorgfaltspflicht kann das Kreditkartenunternehmen auch bereits bezahlte Beträge vom Unternehmen zurückfordern.

Die Polizei empfiehlt:

- Informieren Sie Ihre MitarbeiterInnen über Sicherheitsmerkmale und Zahlencodes der Kreditkarten (Mastercard beginnt zum Beispiel immer mit der Ziffer 5, Visa immer mit 4 usw.)
- Legen Sie klare Regeln für Kreditkartenzahlungen fest, damit Ihre Mitarbeiterinnen und Mitarbeiter Handlungssicherheit haben: Während des Zahlungsvorganges sollten sie nicht ausschließlich die Unterschrift auf der Karte mit jener des Kunden vergleichen, sondern auch die Kartendaten auf Plausibilität prüfen (passt der Name des Karteninhabers zum Kunden, das Geschlecht etc.). Im Zweifelsfall soll die Vorlage eines Lichtbildausweises gefordert werden dürfen. Das ist international durchaus üblich.
- Legen Sie in Ihrem Onlineshop hohe Sicherheitsstandards fest und bieten Sie die Verschlüsselung der Kartendaten Ihrer Kunden an.
- Wenden Sie sich im Schadensfall sofort an das Kreditkartenunternehmen und an die Polizei.
- Stellen Sie der Polizei Bestellunterlagen, Kreditkartenabrechnungen und etwaigen E-Mail-Schriftverkehr zur Verfügung.

Foto: fotolia.de

Scheckbetrug

Die Verwendung gefälschter Schecks zur Bezahlung von im Internet angebotenen Waren und Dienstleistungen.

Was ist passiert?

Auf dem Onlinebuchungsportal meldet sich ein Kunde, der für eine Reisegruppe 30 Doppelzimmer in meinem Hotel bucht. Welche Freude, der Mann verhandelt nicht über Gruppenrabatte und ist bereit, nahezu den gesamten Preis vorab zu bezahlen. Auf seinen Wunsch akzeptiere ich die Bezahlung mittels Scheck. Ich löse den einige Tage darauf einlangenden Scheck bei meiner Bank ein und erhalte prompt den gesamten Betrag gutgeschrieben. Einige Tage später übermittelt mir der Kunde die tragische Nachricht, dass zwei Personen aus der Reisegruppe einen tödlichen Unfall erlitten haben und dass aus diesem Grund die Reise abgesagt werden soll. Er entschuldigt sich für meine Unannehmlichkeiten und ersucht mich, die Buchung zu stornieren und ihm das Geld – freilich abzüglich meiner bereits entstandenen Aufwendungen – mittels Bargeldtransfer an ihn zurückzusenden. Ich behebe 12.000 Euro und sende diese wie besprochen an den Käufer zurück. Zwei Wochen später fordert meine Bank das Geld wieder zurück, da der Scheck gefälscht war. Jetzt habe ich einen Schaden von 12.000 Euro.

Was liegt vor?

Betrüger bestellen diverse Waren und Dienstleistungen, ohne tatsächlich Interesse an dem jeweiligen Angebot zu haben und schicken zur Bezahlung einen gefälschten Scheck. Ihr Ziel liegt darin, den Verkäufer bzw. Geschäftspartner etwa durch das Vortäuschen von Stornogründen möglichst schnell zur Rücküberweisung des Betrages zu bewegen. Sobald die Bank den Scheck als Fälschung erkennt, verlangt sie vom Einreicher den gesamten zur Auszahlung gekommenen Geldbetrag zurück. Somit erleidet der Einreicher einen Schaden in Höhe des Geldbetrages, der an den vermeintlichen Käufer zurück überwiesen wurde.

Die Polizei empfiehlt:

- Überlegen Sie, ob der Kauf Ihrer Ware bzw. die Inanspruchnahme Ihrer Dienstleistung in einem außergewöhnlich hohen Maß plausibel ist.
- Bestehen Sie auf einen sicheren Zahlungsverkehr (z. B. per Kontoüberweisung).
- Lassen Sie sich nicht zu Bargeld-Rücküberweisungen drängen, bevor die Echtheit des Schecks geprüft ist. Die Bankprüfung dauert bis zu drei, eventuell bis zu sechs Wochen. Bis dahin gilt die Auszahlung nur unter Vorbehalt.
- Sichern Sie im Schadensfall den E-Mail-Verkehr und stellen Sie diesen zusammen mit Kopien der Überweisungsbelege der Polizei für die Ermittlungen zur Verfügung.

Foto: fotolia.de

Identitätsbetrug

Die Vorgabe einer falschen Identität bietet Betrügern ein großes Betätigungsfeld. Es reicht vom Kauf eines Mobiltelefons über Bestellbetrügereien bis hin zum groß angelegten Kreditbetrug.

Kontoeröffnungs- bzw. Kreditbetrug

Unter Vorlage falscher Dokumente (Ausweise, Meldenachweise, Gehaltszettel) werden Konten eröffnet oder Kredite beantragt. Die Konten können in der Folge zum Beispiel für illegale Transaktionen genutzt werden. Kredite werden von den Betrügern nicht zurückgezahlt. Die Identitäten können nicht festgestellt werden.

Anmelden von Mobiltelefonen

Bevorzugt wird die Anmeldung von Verträgen unter Verwendung falscher Ausweise, bei denen dem Kunden ein wertvolles Endgerät als gestütztes Produkt gratis überlassen wird. In diesen Fällen generieren meist keine Gesprächsgebühren generiert, sondern das Endgerät weiterverkauft. In manchen Fällen werden Mobiltelefone angemeldet und verwendet, ohne die Kosten zu zahlen, bis das Telefon vom Betreiber gesperrt wird.

Online-Handel

Betrüger bestellen Waren im Internet, wobei sie falsche Daten verwenden oder andere Identitäten annehmen. Die Waren werden vom Betrüger zu einer Ersatzadresse umgeleitet und dort entweder selbst oder von einem „Paketagenten" in Empfang genommen. Den Schaden trägt der Lieferant.

Einmietbetrug

Betrüger mieten – meist unter Vorlage falscher Ausweise – eine Wohnung und haben weder die Mittel noch die Absicht, die Mietkosten zu bezahlen.

Kreditkartenbetrug

Die Betrüger legen zur Bezahlung ihrer Einkäufe (Luxusgüter, Elektronik, Parfums etc.) gefälschte Kreditkarten vor (siehe auch Seiten 18/19). Die Einkäufe erfolgen ohne Inanspruchnahme einer Beratung, gekauft wird meist die größte und teuerste Produkteinheit. Oft verfügen die Betrüger auch über einen gefälschten Ausweis, der zu den Kartendaten passt.

Die Polizei empfiehlt:

- Wenn Sie mit Kunden oder Kundendaten arbeiten, legen Sie Sicherheitsstandards fest, die eine geeignete Identitätsprüfung ermöglichen.
- Lassen Sie sich über IT-Lösungen beraten, die Bonitäts- bzw. Identitätsmerkmale bewerten.
- Wenn Sie Waren versenden, dann bestehen Sie auf einen sicheren Zahlungsverkehr, z. B. per Vorauskasse.
- Bewerten Sie Neukunden kritisch und ermöglichen Sie ihnen keine Lieferung ohne Zahlungssicherheit.
- Stellen Sie der Polizei im Schadensfall Bestell- und Lieferunterlagen bzw. Vertragskopien und Kopien der vorgeblichen Identitätsnachweise zur Verfügung.

Foto: fotolia.de

Inkassobetrug

Die unberechtigten Geldforderungen von angeblichen Anwälten und Inkassobüros.

Was ist passiert?

Über mehrere Monate hinweg erhält unsere Buchhaltung immer wieder Anrufe und Briefe mit der Aufforderung, eine offene Rechnung aus einem Geschäftsfall zu begleichen. Wir haben uns zunächst geweigert, der Forderung nachzukommen, da es kein entsprechendes Geschäft gibt. Mittlerweile hat der angebliche Geschäftspartner ein Inkassounternehmen beauftragt und droht, uns vor Gericht zu bringen, wenn wir nicht bezahlen.

Was liegt vor?

Betrüger geben sich als Rechtsanwälte, Inkassobüros und Ähnliches aus, um von den Opfern Geldforderungen einzutreiben, die in Wirklichkeit unberechtigt sind. Sie fordern beispielsweise die Bezahlung von Kosten für Mehrwert-Telefonie, Geld für den Download kostenpflichtiger Inhalte oder Entschädigungszahlungen wegen Urheberrechtsverletzungen.

Die Polizei empfiehlt:

Zahlen Sie keine Rechnungen, die Sie nicht verursacht haben. Notieren Sie sich die Telefonnummern des Anrufers sowie die Zeitpunkte der Telefonate. Erstatten Sie Anzeige bei der Fernmeldebehörde und der Polizei und stellen Sie die Mahnschreiben sowie die Telefonliste für die Ermittlungen zur Verfügung.

Foto: T. Wengert/pixelio.de

Weitere Betrugsformen

In Kürze: Betrugsarten, die Wirtschaftstreibende ebenfalls kennen sollten.

Frachtbetrug

Die Betrüger treten meist als Firmen aus osteuropäischen Ländern auf und bestellen größere Warensendungen von zum Teil immensem Wert. Die Lieferungen erfolgen oft über renommierte Speditionen. Die Ware wird von den Betrügern umgeleitet und kommt nicht bei jener Firma an, die die Rechnung für die Lieferung erhält. Die Polizei empfiehlt: Unterziehen Sie insbesondere neue Kunden einer Plausibilitäts- und Bonitätsprüfung. Versichern Sie sich der Richtigkeit, wenn ein bestehender Kunde während eines Geschäftsfalles eine Kontodatenänderung bekannt gibt.

Telefonanlagen-Hacking

Vorwiegend nach Geschäftsschluss oder am Wochenende hacken sich Betrüger über ungesicherte Nebenstellen einer Telefonanlage in ein Firmentelefonnetz ein. Die Betrüger vermitteln Telefongespräche über die Anlage, vorwiegend nach Übersee. Die entstehenden immensen Kosten gehen zu Lasten des Unternehmens. Man kann sich davor schützen: Ändern Sie die Standardsicherungen (Passwörter) Ihrer Router, WLAN-Verbindungen und Telefonanlagen, nehmen Sie die Sicherheitsberatung des Herstellers oder Betreibers in Anspruch und wählen Sie sichere Passwörter. Verwenden dabei Sie keine gängigen oder auf die Firma bezogenen Begriffe.

Geldwechselbetrug

Die Betrüger lenken den Kassenpersonal durch Verwirrung und mehrmaliges Hin- und Zurückwechseln verschiedener Stückelungen und Beträge ab und verleiten den Mitarbeiter auf diese Weise dazu, eine höhere Summe aus der Kassa zu geben. Der Fehlbetrag wird meist erst bei der Endabrechnung bemerkt. Häufig wird der Geldwechselbetrug bei Hochbetrieb in Supermärkten, Trafiken und Tankstellen versucht. Profis arbeiten mit der Fingerfertigkeit von Taschenspielern und schaffen es sogar, Bankmitarbeiter zu täuschen.

Herauslocken von Wertcodes

Betrüger versuchen unter Vorgabe einer falschen Identität (z. B. Sicherheitsbeauftragter), Mitarbeiter von Tankstellen, Trafiken und Geschäften telefonisch zur Bekanntgabe von Codes diverser Handy-Ladebons oder Wertbons für den Zahlungsverkehr im Internet zu verleiten. Diese Codes werden von den Betrügern im Internet verwertet oder verkauft. Geben Sie als Geschäftsleiter Ihren Mitarbeitern die Gewissheit, dass weder Sie noch andere Firmenverantwortliche telefonische Abfragen von Wertcodes durchführen. Solche Sicherheitsüberprüfungen existieren nicht! Veranlassen Sie im Schadensfall so rasch wie möglich die Sperre der Codes durch den Betreiber und verständigen Sie die Polizei.

Adressen & nützliche Links

Stadtpolizeikommando Graz
Sauraugasse 1, 8010 Graz
Tel: 059133 65-0
SPK-ST-Graz@polizei.gv.at.at
Notruf:133

GEMEINSAM.SICHER in Graz
059133 65-1312
GemeinsamSicher-ST@polizei.gv.at
www.gemeinsamsicher.at

Kriminalpolizeilicher Beratungsdienst
059133 65-3430
SPK-ST-Graz-KR-FB4@polizei.gv.at

Polizeiinspektion Andritz
Andritzer Reichsstraße 38, 8045 Graz
059133 6581-100
PI-ST-Graz-Andritz@polizei.gv.at.at

Polizeiinspektion Eggenberg
Alte Poststraße 161a, 8020 Graz
059133 6582-100
PI-ST-Graz-Eggenberg@polizei.gv.at.at

Polizeiinspektion Jakomini
Conrad-von-Hötzendorf-Straße 94, 8010 Graz
059133 6583-100
PI-ST-Graz-Jakomini@polizei.gv.at.at

Polizeiinspektion Hauptbahnhof
Europaplatz 7, 8020 Graz
059133 6584-100
PI-ST-Graz-Hauptbahnhof@polizei.gv.at.at

Polizeiinspektion Karlauerstraße
Karlauerstraße 14, 8020 Graz
059133 6585-100
PI-ST-Graz-Karlauerstrasse@polizei.gv.at.at

Polizeiinspektion Kärntnerstraße
Kärntnerstraße 207c, 8053 Graz
59133 6586-100
PI-ST-Graz-Kaerntnerstrasse@polizei.gv.at.at

Polizeiinspektion Lendplatz
Lendplatz 21, 8020 Graz
059133 6587-100
PI-ST-Graz-Lendplatz@polizei.gv.at.at

Polizeiinspektion Liebenau
Liebenauer Hauptstraße 73, 8041 Graz
059133 6588-100
PI-ST-Graz-Liebenau@polizei.gv.at.at

Polizeiinspektion Plüddemanngasse
Plüddemanngasse 37-39, 8010 Graz
059133 6591-100
PI-ST-Graz-Plueddemanngasse@polizei.gv.at.at

Polizeiinspektion Riesplatz
Stiftingtalstraße 3-7, 8010 Graz
059133 6592-100
PI-ST-Graz-Riesplatz@polizei.gv.at.at

Polizeiinspektion Schmiedgasse
Schmiedgasse 26, 8010 Graz
059133 6593-100
PI-ST-Graz-Schmiedgasse@polizei.gv.at.at

Polizeiinspektion Wienerstraße
Wiener Straße 253, 8051 Graz
059133 6594-100
PI-ST-Graz-Wienerstrasse@polizei.gv.at.at

Sicherheitsinformationszentrum Graz (SINFO)

Keplerstraße 25, 8020 Graz
0316 875-5777
office@sinfo.at
www.sinfo-graz.at
facebook.com/sinfograz

GEMEINSAM.SICHER in Graz – Verein

Keplerstraße 25, 8020 Graz
office@gemeinsamsichergraz.at
www.gemeinsamsichergraz.at
facebook.com/gemeinsamsicheringraz

Referat Sicherheitsmanagement und Bevölkerungsschutz der Stadt Graz

Rathaus, Hauptplatz 1, 8011 Graz
0316 872-2261
sicherheitsmanagement@stadt.graz.at
www.sicherheit.graz.at

Wirtschaftskammer Steiermark

Körblergasse 111-113, 8010 Graz
0316 601-0
office@wkstmk.at
wko.at/stmk
Cyber-Security-Hotline: 0800 888 133

Österreichische Nationalbank (OeNB) Zweiganstalt Region Süd

Brockmanngasse 84, 8010 Graz
0316 81 81 81-0
www.oenb.at

www.bundeskriminalamt.at

Offizielle Web-Präsenz des Bundeskriminalamtes Österreich (.BK)
Auch auf Facebook vertreten:
facebook.com/Bundeskriminalamt

Tipp:
Präventionstipps und Cybercrime-Warnungen finden Sie auf der .BK-Webseite unter „Prävention & Opferhilfe“ → „Präventionstipps“ → „Internet kennen“

No More Ransom

Projekt u.a. in Zusammenarbeit mit EUROPOL, bietet Hilfe bei der Entschlüsselung von mittels Ransomware gesperrten Computern.
www.nomoreransom.org

Watchlist Internet

Tagesaktuelle Warnungen und Tipps im Umgang mit Internetbetrug und Online-Fallen
www.watchlist-internet.at

BM.I REPUBLIK ÖSTERREICH BUNDESMINISTERIUM FÜR INNERES .BK REPUBLIK ÖSTERREICH BUNDESMINISTERIUM FÜR INNERES BUNDESKRIMINALAMT

Die Bekämpfung von Internetkriminalität ist ein Schwerpunkt der kriminalpolizeilichen Arbeit.
Sie haben einen Verdacht auf Internetbetrug und benötigen Informationen zur weiteren Vorgehensweise?
Schreiben Sie uns: against-cybercrime@bmi.gv.at

Gut abgeschirmt?

SINFO
Wir wissen's besser.
Sicherheitsinformationszentrum Graz
Keplerstraße 25
Tel. 0316 872-5777
www.sinfo-graz.at
GRAZ STADT GEMEINSAM.SICHER IN GRAZ POLIZEI KRIMINALPRÄVENTION

LUG & TRUG

Wirtschaft Spezial

Wissen und Information zum Schutz vor Betrug

GRAZ

GEMEINSAM.SICHER IN GRAZ

POLIZEI