Kassiere Vorsicht: Internet-Falle!

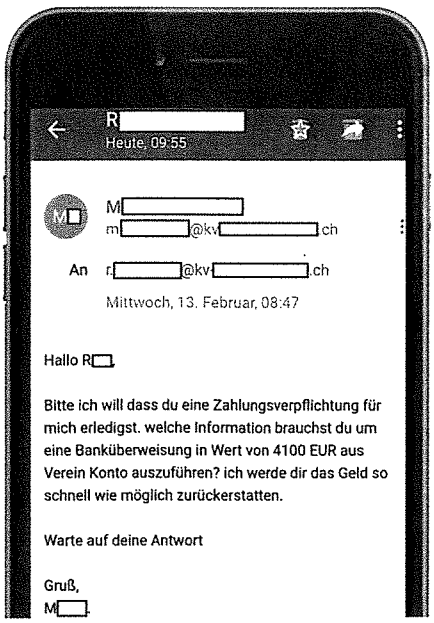
Die Internetkriminalität hat nun auch die kynologischen Vereine erreicht. Mit fingierten Mails – angeblich vom Präsidenten – wurden Kassiere um Veranlassung einer Zahlung gebeten. Bei einer Nachfrage beim Präsidenten kam die Masche dann aber ans Licht. So konnten einige Betrugsversuche vereitelt werden; die Betrüger hatten in Einzelfällen leider auch Erfolg.

Daniel Jung

Cyberbetrug durch falsche internationale Überweisungsaufträge nennt sich das kriminelle Phänomen. Dabei wird meist per Mail mit dem Finanzverantwortlichen eines Unternehmens oder eben eines Vereins Kontakt aufgenommen mit dem Ziel, dass eine internationale Überweisung getätigt wird, welche dann bei der Betrugsorganisation landet.
Solches ist etwa dem kynologischen Verein Frauenfeld widerfahren. So erhielt deren Präsidentin Regula Jung von ihrem Kassier ein Telefonat, ob es zutreffe, dass sie ihm per Mail einen Überweisungsauftrag habe zukommen lassen. «Zuerst war ich gar nicht sicher, weil wir im Zusammenhang mit einem internationalen Anlass tatsächlich etwas in Eurowährung hätten bezahlen müssen. Nachdem mir der Kassier jedoch den Betrag nannte, konnte ich sofort richtigstellen, dass das Mail nicht von mir stammte», so Regula Jung. Auch die Präsidentin der Interessengemeinschaft Nordostschweiz NOV, Gerda Messmer, erfuhr frühzeitig von den Betrugsattacken auf die kynologischen Vereine und sandte umgehend ein Rundmail an alle Vereinspräsidien der NOV. Leider konnten die Betrüger in mindestens einem bekannten Fall dennoch rund 4000 Franken ergaunern.

Die Masche

Die international organisierten Betrüger sammeln mithilfe verschiedener Mittel Informationen über die Vereine. Dies ist relativ einfach; bestehen doch im Internet vollständige Verzeichnisse der Vereinsvorstände mit Namen, Funktion sowie Post- und Mailadressen. Mithilfe dieser Angaben erstellen sie ein neues Mailkonto mit den exakten Angaben des Vereinspräsidiums. Mit einem solchen Mail kontaktieren sie dann die Kassiere und erteilen – angeblich im Namen des Präsidiums – einen entsprechenden Überweisungsauftrag an ein ausländisches Konto.
Fakt ist, dass das Internet den Betrügern dabei hilft, effizient über die Landesgrenzen hinweg zu handeln, an mögliche Opfer zu gelangen und gleichzeitig die Spuren zu verwischen. Wichtig zu wissen ist, dass ein Mailkonto unter einem neuen, schon bestehenden Namen gefälscht hergestellt werden kann. Das ursprüngliche Konto muss dabei nicht gehackt werden. Es gibt leider sehr viele Tools, womit man E-Mail-Adressen verfälschen kann. Nur im Mailheader könnte man erkennen, dass die im Posteingang ersichtliche Mailadresse nur eine «Fassade» ist.



So und ähnlich tönten die E-Mails. Hier gilt: Nicht überweisen, sondern nachfragen. (zvg)

Wer trägt den Schaden?

Haben die Betrüger erfolgreich eine Zahlung ergaunert, so stellt sich die Frage, wer den Schaden trägt. Grundsätzlich wurde die Überweisung in den geschilderten Fällen zu Lasten des Vereinskontos getätigt und dieser ist primär geschädigt. Kann nun der Verein den Betrag, welchen der Kassier fälschlicherweise zu Lasten des Vereins überwiesen hat, zurückfordern? Grundsätzlich haften Vorstandsmitglieder, so auch Kassiere, gemäss Auftragsrecht für eine sorgfältige Ausführung ihrer Aufgaben (dies hat nichts zu tun mit dem Haftungsausschluss der Vereinsmitglieder für Verbindlichkeiten des Vereins!). Kann dem Kassier demzufolge nachgewiesen werden, dass er über die Betrugsmasche bereits vorgängig informiert worden war und das gefälschte Mail bei einigermassen gründlicher Prüfung auf einen genügenden Verdacht hätte schliessen lassen müssen, so wäre eine Haftung zu prüfen.

Information und Strafanzeige

Als Sofortmassnahmen nach Erhalt eines Betrugsmails sind Information an weitere mögliche Betrugsopfer und eine Strafanzeige bei der Polizei angezeigt. Nur wer ungenügend informiert und zu wenig aufmerksam ist, kann betrogen werden. Deshalb ist ganz wichtig, über alle möglichen Kanäle alle wichtigen Organe, insbesondere Vereinspräsidien und Vereinskassiere, über die erhaltene Betrugsmasche zu informieren. Zudem ist eine Strafanzeige bei der Polizei sinnvoll, damit diese koordiniert gegen die Betrüger vorgehen kann. Leider sind bei der Cybercrime die meisten örtlichen Polizeidienststellen noch zu wenig informiert, weshalb das Bundesamt für Polizei (fedpol)

Hereingefallen? In den vergangenen Monaten erhielten zahlreiche Kassiere betrügerische E-Mails. (Lucia Romero / www.shutterstock.com)

ein entsprechendes Meldeformular zur Verfügung stellt. Dieses kann im Internet direkt heruntergeladen und online ausgefüllt werden. Auf der Website des fedpol befinden sich auch weitere nützliche Informationen zu Cybercrime.

Vorsichtsmassnahmen

Wie kann man sich gegen das Vorgehen der Betrugsbanden schützen? «An erster Stelle steht der Verdacht», lautet ein kriminalistischer Grundsatz. Man tut gut daran, Mails, welche einem zur Aufforderung einer Zahlung oder Bekanntgabe von Daten auffordern, gut anzuschauen. Die Sprache und auffällige Details verraten den falschen Absender oft. Wenn in einem Mail einer Präsidentin, welche sonst in gutem Deutsch kommuniziert, «ich möchte dass du ein Überweisung machen» steht, so ist das schon mal verdächtig. Ein findiger Kassier, welcher wusste, dass sein Vereinspräsident kein iPhone besitzt, wurde auf den Vermerk «von meinem iPhone gesendet» hellhörig und fragte beim Vereinspräsidenten nach. Generell sollte man sich vor Überweisung einer Zahlung oder Bekanntgabe geschützter Daten auf einem anderen Informationskanal rückversichern.

Immer zuerst nachfragen

Die Vereinigung schweizerischer Kriminalprävention empfiehlt zur Verhinderung des Cyberbetrugs folgendes:

- Keine weitere Kommunikation mit der verdächtigen Mailadresse, weil damit der betrügerische Absender weitere Informationen erhält.
- Erkundigung beim Auftraggeber über einen anderen Kanal (telefonisch, per SMS), ob der Auftrag wirklich von ihm stamme.
- Auf die Rechtschreibung und Besonderheiten des vermutlich gefälschten Mails achten.
- Plausibilität des angeblichen Auftrags beim Präsidium oder anderen Vorstandsmitgliedern abklären. In der Regel sollte ja für eine Zahlungsüberweisung von mehreren tausend Franken in ausländischer Währung ein Vorstandsbeschluss vorliegen, an welchem der Kassier mitgewirkt hat oder mindestens darüber vorgängig orientiert worden sein sollte.

Fazit: Die Betrugsbanden werden immer raffinierter und sind mit besten technischen Mitteln ausgerüstet. Mit den nötigen Vorsichtsmassnahmen sollte es jedoch möglich sein, sich vor unnötigem Schaden zu bewahren.

Nützliche Links im Internet: www.fedpol.admin.ch/fedpol/de/home/kriminalitaet/cybercrime/meldeformular.html und www.skppsc.ch/de/themen/internet/internet-cyberbetrug/

Zum Autor
Daniel Jung ist Rechtsanwalt und spezialisiert auf Rechtsfragen rund um die Hundehaltung. Er besitzt selber einen Deutschen Schäferhund. Internet: www.daniel-jung.ch