

Millionenschäden durch Manipulation von -mittels E-Mail-versandten Rechnungen

12.06.2024, 17:48 | Handel, Wirtschaft, Finanzen, Banken & Versicherungen

Pressemitteilung von: *LSS Rechtsanwälte*

LSS Rechtsanwälte informieren BaFin über gegenwärtig auffällig häufige Involvierung des FinTechs "bunq"

Gegenwärtig werden zahlreiche Betrugsfälle in der Kanzlei LSS Rechtsanwälte gemeldet, bei denen Verbraucher oder Unternehmer auf gefälschte Rechnungen Geldbeträge überweisen. Zumeist werden Rechnungen, die Lieferanten oder Handwerker tatsächlich per E-Mail an die späteren Geschädigten übersenden von den Tätern abgefangen und ausschließlich im Hinblick auf die Bankverbindung geändert. Die Täter öffnen das Rechnungs-pdf und ersetzen mittels Software die korrekte IBAN des Ausstellers gegen eine andere IBAN, die den Tätern zuzurechnen ist. Die E-Mail wird dann -solcherart verfälscht- in das Postfach der späteren Geschädigten verschoben oder aber mittels einer ebenfalls gefälschten E-Mail-Adresse versendet.

Begann diese Betrugsmasche noch vor einiger Zeit mit auffälligen ausländischen Bankverbindungen (IBAN mit ausländischer Länderkennung) und waren hieran ggf. noch zu erkennen, so sehen wir derzeit sehr häufig deutsche IBANs (Länderkennung DE), warnt der Frankfurter Fachanwalt für Bankrecht Matthias Schröder (LSS Rechtsanwälte). Das niederländische Fintech "bunq" wirbt zum Beispiel damit, dass man in Minutenschnelle online eine Bankverbindung mit gleich mehreren deutschen IBANs bei ihm eröffnen könne. Dies scheinen sich die Täter zu Nutze zu machen, denen zusätzlich mutmaßliche generelle Schwächen bei der Online-Identifikation zur Kontoeröffnung zu pass kommen. Zum Erfolg der Masche trägt noch die wenig bekannte Tatsache, dass Banken den angegebenen Namen des Kontoinhabers seit Einführung der IBAN nicht mehr prüfen, bei. Die Geschädigten geben also bei der Überweisung den auf der verfälschten Rechnung noch korrekt angegebenen Kontoinhaber und Empfänger (z.B. ein Autohaus) an und aber die verfälschte IBAN der Täter. Statt bei z.B. bei Commerzbank landet das Geld dann z.B. bei "bunq" und wird von den Tätern nach Geldeingang weiterüberwiesen, zumeist in das Ausland. Bis der Schwindel auffliegt vergehen oft Tage. Ein Überweisungsrückruf ist nach hiesiger Erfahrung gegenwärtig in gut 1/3 der Fälle noch erfolgreich, da einige der betroffenen Banken mittlerweile simple Algorithmen einsetzen (neues Konto, sofortige hohe Geldeingänge und direkte Weiterüberweisung = Verdachtsfall). Manche Banken scheinen solche Erwägungen und Prüfungen selbst bei sechsstelligen Überweisungen gar nicht erst anzustellen.

Was hinter den Angriffen wirklich steht, bleibt oft unklar. Bei dieser Betrugsmasche hacken sich die Täter in den E-Mail-Server des Verkäufers oder des Käufers oder fangen die E-Mail auf anderem Weg ab und greifen dabei Zahlungsdetails ab. Im Anschluss versenden die Täter eine E-Mail, die scheinbar von dem Verkäufer stammt, ändern hingegen die Bankverbindung, an die die offene Kaufpreiszahlung gezahlt werden soll. Da die Rechnung ansonsten täuschend echt aussieht, überweist der Käufer an die falsche Bankverbindung. Erst wenn dann der Käufer vom Verkäufer eine Mahnung wegen fehlender Zahlung erhält, fällt der Betrug auf. Doch dann ist es meist schon zu spät und der Kontoinhaber des lediglich vermeintlich richtigen Kontos nicht mehr greifbar.

Praxishinweis: Um zu verhindern, Opfer dieser Betrugsmasche zu werden, empfiehlt LSS Rechtsanwälte vor der Zahlung auf eine per E-Mail erhaltene höhere Rechnung die angegebene Kontoverbindung dahingehend zu überprüfen, ob die E-Mail tatsächlich von dem Verkäufer stammt, ob die angegebene Kontoverbindung tatsächlich zum Verkäufer gehört. Über einen IBAN-Rechner im Internet kann man die Bank hinter einer IBAN leicht ermitteln. Im Zweifel sollte man mit dem Rechnungsteller einen Abgleich telefonisch durchführen.

LSS Rechtsanwälte unterhält im Dezernat Bankrecht seit mehr als 20 Jahren eine Spezialisierung für Zahlungsbetrug und setzt sich für die Rückholung der Gelder ein.

LSS Rechtsanwälte

Kaiserhofstr. 10
60313 Frankfurt

Matthias Schröder

06921936560

schroeder@lss-partner.de

<http://www.lss-partner.de>

News-ID: 1263524 • Views: 341 (Stand: 21.10.2026)

Link zur Pressemitteilung:

<https://www.openpr.de/news/1263524/Millionenschaeden-durch-Manipulation-von-mittels-E-Mail-versandten-Rechnungen.html>