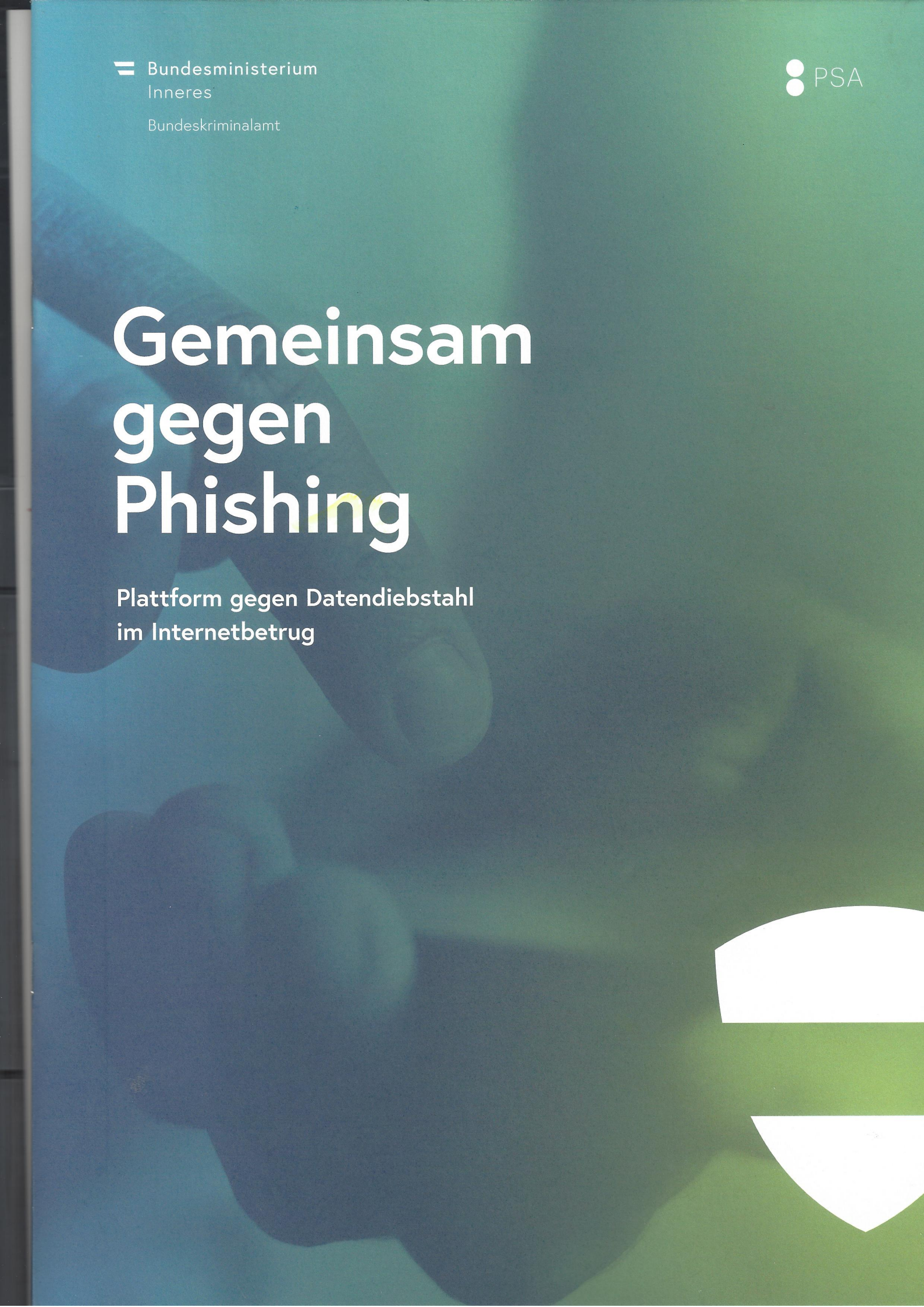
Bundesministerium
Inneres

Bundeskriminalamt

PSA

Gemeinsam gegen Phishing

Plattform gegen Datendiebstahl im Internetbetrug



KOMMUNIKATION & VERHALTEN

„Opfer sind nicht dumm."

Warum funktioniert Phishing? Wirtschaftskriminal- und Verhaltensanalytikerin Patricia Staniek erklärt im Interview die Hintergründe von Social Engineering.

Wie funktioniert Social Engineering aus Sicht der Verhaltensanalyse?
Staniek: Amateure hacken Systeme – Profis hacken Menschen: Darum geht es beim Social Engineering. Phishing-Betrüger arbeiten mit Zeitdruck, bauen also die Dringlichkeitsfalle ein. Sie nutzen Angststrategien, um Menschen zu schnellen Handlungen zu bewegen. Sie zielen darauf ab, persönliche Informationen wie Passwörter, Kreditkarteninformationen oder Bankdaten von ahnungslosen Empfängern zu erwirken. Was passiert, kann man als „Brainfucking" bezeichnen.

„Amateure hacken Systeme – Profis hacken Menschen."
Bruce Schneier

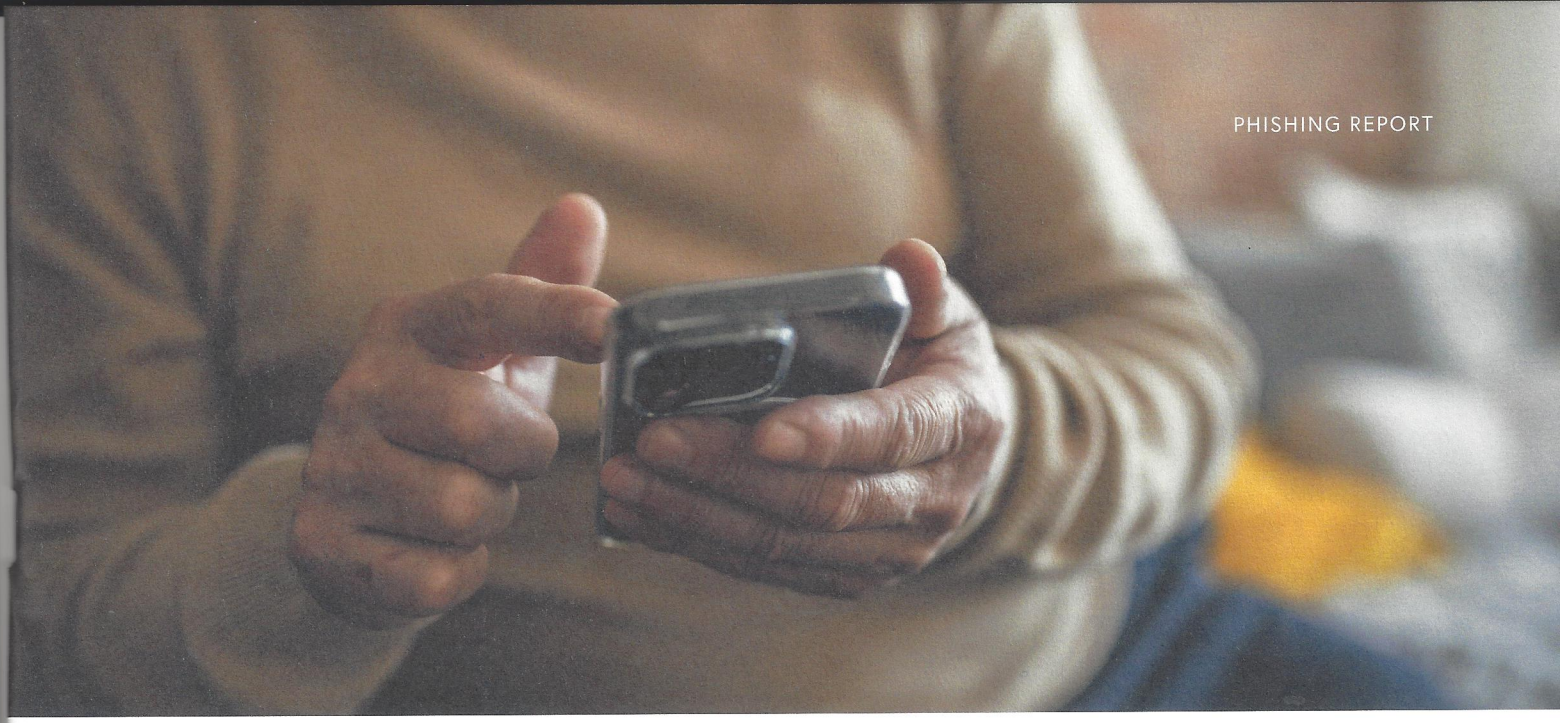
Warum funktioniert das?
Staniek: Die Betrüger sind oft psychologisch geschult und verwenden vorgefertigte Gesprächsleitfäden. Sie wissen genau, welche Taktik sie einsetzen müssen, um die Opfer in die Zielrichtung zu bewegen, um diese letztendlich vollkommen skrupellos abzuzocken.

„Die meisten Opfer sind nicht dumm. Sie kennen lediglich die Betrugsmethoden nicht."

Der Mensch muss sich nicht vor der Technologie fürchten, sondern vor der Strategie. Die meisten Opfer sind nicht dumm. Sie kennen lediglich die Betrugsmethoden nicht. Wer weder die Betrugsform noch die Betrugsmethode kennt, lässt sich leicht über den Tisch ziehen.

Was ist aus Ihrer Sicht für die Prävention wichtig?
Staniek: Eigensicherheit ist ein wichtiges Thema. Prävention funktioniert dann, wenn wir nicht über etwas reden, sondern mit jemand reden – mit den Zielgruppen. Jeder hat eine Tante oder eine Oma oder andere, die betroffen sein können.

Nicht nur Naivität und Leichtgläubigkeit, auch autoritätshörige „People Pleaser" und wenig internet- oder handyaffine Menschen sind gefährdet. Phisher und Hacker haben gute, geschulte Menschenkenntnisse. Sie wissen, was zu tun ist, wenn ein Opfer am Telefon so oder so reagiert.



Welche Ansatzpunkte sind im Kampf gegen Phishing wichtig?
Staniek: Wir brauchen erstens Sensibilisierung, Aufklärung und Schulung. Umfassende Schulungen für Mitarbeiter und die Öffentlichkeit sind entscheidend, um das Bewusstsein für Phishing-Angriffe zu schärfen.

Zweitens geht es um technologische Lösungen. Innovative Sicherheitslösungen, wie Anti-Phishing-Tools und E-Mail-Authentifizierungstechnologien, sind unerlässlich. Ein Vorteil der Künstlichen Intelligenz: Sie kann helfen, Muster von Phishing-Angriffen zu identifizieren.

Und drittens ist Zusammenarbeit und Infosharing zentral. Eine enge Zusammenarbeit zwischen Unternehmen, Behörden und Sicherheitsexperten ist von entscheidender Bedeutung für schnellere Reaktionen und präventive Maßnahmen.

Was konkret bringt die bessere Zusammenarbeit im Kampf gegen Phishing?
Staniek: Eine verbesserte Zusammenarbeit im Kampf gegen Phishing birgt zahlreiche Vorteile. Erstens ermöglicht sie einen effektiven Informationsaustausch über aktuelle Bedrohungen und Angriffsmuster.

Zweitens fördert sie die Entwicklung und Implementierung gemeinsamer Sicherheitsstandards, die die Widerstandsfähigkeit gegenüber Phishing erhöhen.

Mag. Patricia Staniek
Wirtschaftskriminal- und Verhaltensanalytikerin, BSc Betriebswirtin für Wirtschaftskriminalistik/-kriminologie, Certified Master Profiler & Ausbildnerin, Akademische Expertin für internationale Sicherheitsmanagements

„Prävention funktioniert dann, wenn wir nicht über etwas reden, sondern mit jemand reden – mit den Zielgruppen."

Drittens ermöglicht sie eine koordinierte Nutzung von Ressourcen und Expertise, um innovative Lösungen zu entwickeln. Insgesamt schafft eine verbesserte Zusammenarbeit eine robustere Verteidigung gegen Phishing-Angriffe, was sowohl Unternehmen als auch die breite Öffentlichkeit schützt.

Gemeinsam gegen digitale Bedrohungen

Im Rahmen der Auftaktveranstaltung zur Plattform gegen Datendiebstahl im Internetbetrug diskutierten unter der Leitung von Thomas Von der Gathen (PSA Payment Services Austria GmbH), Verhaltensanalytikerin Patricia Staniek, Head of Fraud-Management Birgit Langeder (Erste Bank), Bundeskriminalamt-Experte Mohamed Ibrahim (Cybercrime Competence Center C4) und CSO Wolfgang Schwabl (A1 Telekom Austria AG und Vorsitzender CSP des BKA) gemeinsame Antworten auf die Phishing-Gefahr.

Head of Fraud-Management **Birgit Langeder** von der Erste Bank erklärte, dass man die gruppenweiten Maßnahmen der Banken zur Vermeidung von Betrug nicht unterschätzen dürfe. Neben der verpflichtenden Zwei-Faktor-Authentifizierung wurden auch Fraud-Management-Systeme etabliert, um Schäden für Kunden und Institute zu verhindern. Neben der Schaltung von Warnhinweisen und einem Warning-Screen bei gleichzeitigem Telefonieren und Online-Bankgeschäften betonte Langeder auch die gute Zusammenarbeit mit Watchlist Internet. Die gesetzten Maßnahmen kämen bei den Kundinnen und Kunden sehr gut an.

Langeder unterstrich die Wichtigkeit der Zusammenarbeit zwischen Banken und Polizei. Man versuche, die Kunden überall zu erreichen und zu sensibilisieren.

Zusammenarbeit unterstützt Prävention

Bundeskriminalamt-Experte **Mohamed Ibrahim** (Cybercrime Competence Center) nannte als Herausforderungen bei der Bekämpfung von Internetbetrug die Komplexität des Themas, internationale Hürden bei der Zusammenarbeit und die hohe Zahl von Anzeigen. Den aktuell 28.000 Anzeigen pro Jahr stehe eine noch höhere Dunkelziffer gegenüber. Der Großteil betreffe Phishing. Ziel müsse es sein, durch bessere Prävention Fälle zu verhindern. Die Zusammenarbeit mit Banken und Mobilfunkanbietern und die gemeinsame Plattform gegen Phishing helfe, mehr in die Prävention zu investieren, betonte der Bundeskriminalamt-Experte.

Wissen über Opfer wichtig

Verhaltensanalytikerin **Patricia Staniek** sprach sich dafür aus, Menschen noch besser zu informieren. Kein Polizist holt an der Haustür Geld und Schmuck ab. Die potenziellen Opfer müssen auf allen möglichen Ebenen erreicht werden, durch Medien, durch Institutionen, Vereine und Familienangehörige.

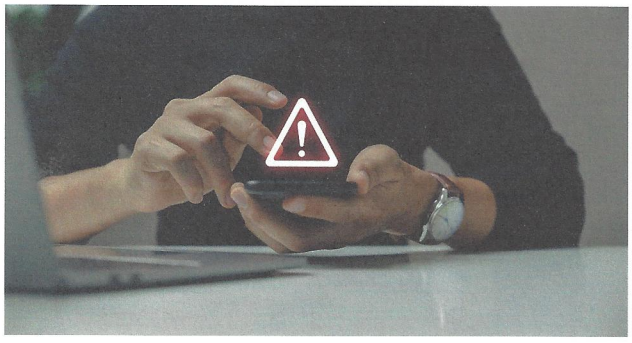
Letztlich könne man in der Prävention Menschen nur erreichen, wie es die Täter selbst bei Social Engineering tun – „in ihr Gehirn einsteigen". Man müsse wissen, wie Opfer ticken, um Präventivmaßnahmen richtig weiterzuentwickeln.

Bild v. l. n. r.: Wolfgang Schwabl, Mohamed Ibrahim, Thomas Von der Gathen, Patricia Staniek, Birgit Langeder

Rechtliche Weiterentwicklung nötig

Wolfgang Schwabl, CSO A1 Telekom Austria AG und Vorsitzender der Cyber Sicherheit Plattform des Bundeskanzleramtes, machte in der Diskussion auf rechtliche Lücken aufmerksam: Es sei den Telekom-Anbietern nicht erlaubt, Phishing-SMS zu stoppen, weil das Telekom-Gesetz dies nicht erlaube.

Die rechtliche Regelung, die sich am traditionellen Briefgeheimnis orientiert, sei nicht mehr zeitgemäß. Die Kommunikation laufe schließlich nicht mehr – wie per Brief und Telefon – von Mensch zu Mensch. SMS würden heute von Computerprogrammen versendet. Angesichts dieser maschinengenerierten Attacken müsse man den Rechtskontext überlegen, sagte Schwabl: „Ist nicht der Schutz der Empfänger vor bösartigen Nachrichten wichtiger?" Er verwies auf die Notwendigkeit eines breiten gesellschaftlichen Konsenses in dieser Frage.



Im Bereich alphanumerischer SMS biete das Urheberrecht einen Ansatz für mehr Schutz. Noch besser wäre allerdings eine Registrierungspflicht für alle alphanumerischen Absender. Für diese Frage brauche es jedenfalls einen Konsens zwischen Parteien und Behörden. Man werde das Gespräch in diesem Sinn weiter vertiefen, kündigte der Vorsitzende der Cyber Sicherheit Plattform des Bundeskanzleramtes an.

Zusammenarbeit weiterführen

Bundeskriminalamt-Experte **Mohamed Ibrahim** unterstrich abschließend die Wichtigkeit von Anzeigen: Mit jeder Anzeige könne man Verbindungen herstellen. Es gebe immer wieder Ermittlungserfolge.

Head of Fraud-Management **Birgit Langeder** wünschte sich, dass die Zusammenarbeit mit Polizei und Banken weitergeführt werden soll. Auch sie plädierte für rechtliche Weiterentwicklungen, um den Austausch zu verbessern. Derzeit würde dies der Datenschutz noch behindern.

Es gebe allerdings Bemühungen, dies zu verbessern. Der legale Austausch sei wichtig, damit nicht noch mehr Geld in organisierte Kriminalität fließe, sagte die Expertin.

Auch Verhaltensanalytikerin **Patricia Staniek** begrüßte die forcierte Zusammenarbeit. Großes Ziel sei die Eigensicherheit der Menschen.