

«Passwörter sind wie Zahnbürsten, die man mit niemandem teilt»

Spannende Einblicke der Schwyzer Polizei in die grassierende Internetkriminalität – und was man dagegen tun kann.

Franz Steinegger

Zwei Spezialisten der Kantonspolizei gaben am Mittwochabend im Rahmen eines Vortrages der Volkshochschule Schwyz Einblick in die grassierende Internetkriminalität. Thomas Hürlimann von der Dienststelle Prävention hielt gleich zu Beginn fest: «Es kann jeden und jede treffen.»

Er veranschaulichte dies an einigen konkret vorgefallenen Ereignissen, wo selbst gebildeten Menschen Hunderttausende von Franken von ihren Konten und einen ganzen Tresor voller Schmuck vor ihren Augen «abgezügelt» wurden.

Die Betrüger sind psychologisch gut geschult

Seine aus der Praxis stammenden Schilderungen zeigen, dass niemand vor den gut organisierten Banden gefeit ist. Der Einstieg in dieses verlustreiche Geschäft ermögliche zu 99 Prozent der Geschädigte selbst. «Die Kriminellen versuchen, den Finger zu greifen. Wenn sie einmal erfolgreich angedockt haben, läuft alles wie von selbst ab, bis die Täter die ganze Hand haben.»

Die psychologisch gut geschulten Anrufer «dringen ins Hirn ein und schaffen es, selbst intelligente Menschen zu manipulieren», erklärte der Spezialist, der seit sechs Jahren im Auftrag der Kantonspolizei auf Vortragsreise ist. «Mündige Menschen werden dazu gebracht, freiwillig und ohne äusserlichen Druck Geld zu überweisen.»

«Wir sind gläserne Menschen»

Die Betrüger gehen stets nach dem gleichen Muster vor: Sie offerieren geschickt ein «leuchtendes» Angebot, «das man nicht überbieten kann», wie es Hürlimann formulierte. Damit lege



Thomas Hürlimann (links) und Stefan Kudzielka beantworteten im Anschluss an ihr spannendes Referat persönliche Anliegen der Gäste. Bild: Franz Steinegger

die Täterschaft einen Schatten über das Urteilsvermögen der Zielperson. Vielfach würden «Wünsche, Bedürfnisse und Ängste» der Betroffenen bewirtschaftet.

Das beginne oft mit kleinen Dingen. «Mit täuschend echten, aber falschen Fakten schüren sie in einem weiteren Schritt Ängste, dringen damit ins Hirn ein und fordern zur Geheimhaltung auf, womit die Geschädigten gegenüber Hilfe von aussen blockiert werden.»

«Die organisierte Kriminalität hat gigantische Ausmasse angenommen», unterstrich Stefan Kudzielka von der Fachstelle Cybercrime der Kantonspolizei Schwyz. Die Betrügerbanden seien professionell aufgestellt mit Hunderten von Leuten im Hinter-

grund – Anwälte, Psychologen, IT- und Finanzspezialisten. Er präzierte: «Wir sind gläserne Menschen und hinterlassen täglich unseren digitalen Fussabdruck» – durch Mails, Suchmaschinenanfragen, Formularregistrierungen, Login-Daten, Hochladen von Dateien, Postings oder Chats in sozialen Netzwerken.

«KI wird unsere Gesellschaft grundlegend erschüttern»

Schlagwörter werden herausgefiltert, Daten aufbereitet, und es wird auch gehandelt. «Die Betrüger wissen, wer sich mit was beschäftigt und kennen sich in der Mentalität der Schweizer aus.» Mit diesem Wissen gehen sie gezielt auf die Schwachstellen der Menschen los. Das nennt man «social hacking».

Fünf Schritte zur digitalen Sicherheit

Die Kantonspolizei Schwyz gibt folgende Empfehlungen zur digitalen Sicherheit:

- Sichern Sie Ihre Daten regelmässig auf einer externen Festplatte.
- Nutzen Sie ein Virenschutzprogramm und aktivieren Sie dessen automatische Update-Funktion.
- Aktivieren Sie die automatische Update-Funktion für das Betriebssystem und alle installierten Programme und Apps.
- Verwenden Sie sichere Passwörter mit mindestens 10 Zeichen aus Ziffern, Gross- und Kleinbuchstaben sowie Sonderzeichen. Wer sicher sein will, erhöht diese Kombination auf bis zu 18 Zeichen, weil in den letzten Jahren die Entschlüsselung von Passwörtern ra-

sante Fortschritte gemacht hat. Man kann gut verschlüsselte Passwörter zum Beispiel durch einen Spruch wie folgt zusammenstellen: «Meine Tochter Tamara Fabienne Meier hat am 19. Januar Geburtstag!», was folgendes Passwort ergibt: MTTFMha19.JG!.

– Seien Sie beim Surfen im Internet stets misstrauisch. Dienstleister wie Finanzinstitute oder Telekommunikationsunternehmen fragen nie nach einem Passwort, weder per Mail noch per Telefon. Und sie verlangen auf diese Weise auch keinen Passwortwechsel.

Für aktuelle Betrugsmaschen (beispielsweise beim Kauf der E-Vignette) und vertiefte Informationen zur Thematik empfiehlt die Polizei die stets aktualisierte Internetadresse www.cybercrimepolice.ch.

Es sei ein «Fischen im Meer der Gesellschaft», ergänzte Thomas Hürlimann. Das werde mit der künstlichen Intelligenz (KI) weiter perfektioniert, sodass man am Schluss nicht mehr Wahres von Falschem unterscheiden könne. «KI wird unsere Gesellschaft grundlegend erschüttern, weil man nicht mehr Richtig von Falsch unterscheiden kann. Das katapultiert uns zurück in die Unwissenheit.»

«Bei Unsicherheiten müssen Sie sich rückversichern, bevor es zu spät ist», warnte Stefan Kudzielka. Ein absolutes No-Go sei die Preisgabe von Passwörtern und Kontoinformationen. «Passwörter sind wie Zahnbürsten, die man mit niemandem teilt», brachte es der IT-Spezialist auf den Punkt. «Die besten Sicherheitstechnologien nüt-

zen nichts, solange die Schwachstelle Mensch nicht gesichert ist.»

Basis jeden Betrugs sei, Vertrauen aufzubauen und dann Ängste zu schüren. «Angst in Kombination mit Vertrauen eliminiert rationales Denken», weiss Stefan Kudzielka aus vielen konkreten Fällen.

Kritisch Hinterfragen und aufs Bauchgefühl hören

Als Gegenmittel empfiehlt er, Klarheit zu schaffen und das eigene Bewusstsein zu stärken: kritisches Hinterfragen, nicht einer vorgetäuschten Obrigkeit blind folgen, auf das Bauchgefühl hören und das Gefühl mit dem Verstand überprüfen. «Halten Sie fremde Menschen auf Distanz», riet der Experte Kudzielka.