

# Cyber Crime – die dunkle Seite der Digitalisierung

Forum des Informationskreises der Wirtschaft Traun/Alz zeigt perfide Tricks der Kriminellen und ihre Bekämpfung

**Nußdorf.** „Cyber Crime“ – die Schattenseite der Digitalisierung stand im Mittelpunkt des jüngsten Forums beim Informationskreis der Wirtschaft (IdW) Traun/Alz, moderiert von Vorstandsmitglied Stefan Neumann. Die Experten zur Bekämpfung und Vorbeugung der Internet-Kriminalität, Kriminaloberrat Oliver Penonic (Leiter des Cyber Crime Centers im Münchner Polizeipräsidium), Oberstaatsanwalt Wolfgang Giese (Leitender Oberstaatsanwalt Traunstein) sowie Franz Obermayer (Inhaber der auf IT-Sicherheit spezialisierten Unternehmen FOXiT und Compliment AG aus Kirchweidach) standen Rede und Antwort. Gastgeber des Forums war die Spedition Eberl in Aying in Nussdorf bei Traunstein.

Welche Dimensionen die Kriminalität im noch jungen Zeitalter der Digitalisierung erreicht hat, illustrierte Oliver Penonic vom Cyber Crime Center der Kripo in München. Das ebenfalls noch junge Dezernat kombiniert die Arbeit von Informatikern mit klassischer Ermittlerarbeit der Polizei, baut auf die Erfahrung langjähriger Experte im Fach, die bis in das Zeitalter der ersten btx-Systeme in den späten 70er Jahren zurückreicht, nutzt Erfahrungsaustausch in Hacker-Foren und Messen mit Internet-Freaks.

Das Netz und seine Macher, selbst die Basis für das in jüngster Zeit arg in Verruf geratene Darknet seien nicht von Grund auf böse, betonte der Fahnder, aber es werde zunehmend von professioneller und organisierter Kriminalität gekapert, um illegales Geld zu erwirtschaften – zum Schaden anderer.

Das Spektrum ist weit gefasst, vom Handel mit illegalen Gütern wie Waffen und Drogen über Kinderpornografie bis zu Erpressung, Geldwäsche und dem Abgreifen von Daten. Gerade in diesem Fall lieferten sich Kriminelle oft ein Kopf-an-Kopf-Rennen selbst mit der Gesetzgebung, denn oftmals seien nicht mal die rechtlichen Kriterien, was erlaubt ist und was nicht,



**Experten für die Verhinderung und Bekämpfung von Internetkriminalität (Cyber Crime) beim Forum des Informationskreises der Wirtschaft (IdW) bei der Spedition Eberl. Im Bild von links; Kriminaloberrat Oliver Penonic (Leiter des Cyber Crime Centers im Münchner Polizeipräsidium), Oberstaatsanwalt Wolfgang Giese (Leitender Oberstaatsanwalt Traunstein) sowie Franz Obermayer (Inhaber der auf IT-Sicherheit spezialisierten Unternehmen FOXiT und Compliment AG aus Kirchweidach)** – Fotos: ede



**Stefan Neumann**

klar definiert.

Rund 300 000 neue Viren infizieren täglich das Internet, informierte Oliver Penonic; 30 Milliarden Spam-Mails werden jeden Tag im Internet verteilt. Mit zigtausend neuen infizierten Internetseiten täglich kalkulieren die Experten; rund 150 000 „Malwares“, also Schadprogramme allein für Smartphones werden geschätzt. Und letztendlich ein Schaden von rund 445 Milliarden US-Dollar entsteht laut Penonic jedes Jahr durch Kriminalität im Internet und mit Hilfe des Internets (Cyber Crime).

Als eine der jüngsten Attacken haben sich offenbar in Bewerbungen versteckte Schadprogramme erwiesen. Die Masche: Auf ausgeschriebene Stellen bewerben sich trickreiche Betrüger online mit perfekt fingierten Anschreiben, mit Dateien im Anhang, die gewissenhaft den Bewerber beschreiben und

die Neugierde wecken, sich noch mehr Nachweise, gerne auch in einer Cloud, anzusehen und dabei selbst für einen Fachmann oft kaum zu erkennende Schadprogramme einschleusen. Wird die schädliche Software aktiv, dann werden die Computer und vor allem die darauf enthaltenen Daten der Opfer lahmgelegt und erst nach Überweisung von Lösegeld wieder freigegeben.

Oliver Penonic schilderte die Entwicklung zwischen Ermittlern und Kriminellen als einen harten Wettlauf. Zusätzliche Herausforderung für Polizei und Staatsanwaltschaft, so bestätigte auch Leitender Oberstaatsanwalt Wolfgang Giese: Die Täter sitzen oft im Ausland – von der Ukraine bis ins ferne China. Und abgesehen von den Sprachbarrieren und unterschiedlichen Rechtssystemen zeige sich auch die unterschiedliche Mentalität oder gelegentliche Nonchalance in der Strafverfolgung als Barrieren.

Trotz der Hürden sei es kein aussichtsloser Kampf, betonten Polizist und Staatsanwalt. Auch auf der Seite der Legalität entwickeln sich Partnerschaften und Netzwerke, um den kriminellen

Machenschaften zu Leibe zu rücken. So gebe ins inzwischen erfolgreiche Kooperationen mit Kollegen in Russland und in Rumänien, um dort Spuren zu verfolgen und nach Tätern zu fahnden.

Die Diskussion mit Unternehmen aus der Region zeigte, dass regionale Unternehmen vor kriminellen Aktionen mit Hilfe und über das Internet, durch Datenklau und Betrug nicht gefeit sind. Den krasssten Fall hatte es vor rund zwei Jahren im benachbarten Oberösterreich gegeben. Dort wurden über einen vorgeblichen Auftrag eines Konzernchefs (fake presidency fraud) 50 Millionen Euro für eine vermeintliche Unternehmensübernahme an Betrüger überwiesen und schnell auf andere Konten weiterverteilt, so dass das Unternehmen auf einem enormen Schaden sitzen blieb.

Von ähnlichen Versuchen und Attacken, wenngleich nicht mit ganz so hohem Schaden, berichtete Penonic auch für Unternehmen in Oberbayern. Zwar sei es der Polizei gelungen, etliche Millionen zurückzuholen, allerdings hätten die Kriminellen in der jüngsten Vergangen-

heit ihre Methoden so verfeinert, dass viele Millionen unwiderbringlich verloren seien.

Die Zahl der bekannt gewordenen Fälle von Internet-Kriminalität im Bereich der Staatsanwaltschaft Traunstein bezifferte Wolfgang Giese für das vergangene Jahr auf rund 100 Fälle im Vergleich zu rund 40 000 Fällen konventioneller Kriminalität und rund 106 000 Verfahren wegen Delikten im Kontext mit dem Ausländerrecht.

Die Staatsanwaltschaft stellt sich jedoch auf den neuen Trend ein, bildet Kompetenzzentren und baut die Kooperation mit den Fachdezernaten der Kriminalpolizei, mit dem Landes-LKA) und dem Bundeskriminalamt (BKA) aus.

Einen pragmatischen Ansatz, um sich gegen die Gefahren aus dem Internet zu wappnen, beschreibt Sicherheitsexperte Franz Xaver Obermayer mit dem Zitat: „Es ist besser, Deiche zu bauen, als darauf zu hoffen, dass die Flut allmählich Vernunft annimmt.“ Obermayer, seit über 20 Jahren Experte für maßgeschneiderten Schutz und lizenzierte Auditor nach den ISO-Normen „27 x“, rät zum Aufbau und zur Implementierung von angemessenen Informationssicherheitsmanagementsystemen (ISMS) und die Schulung der Mitarbeiter.

Sicherer Umgang mit Passwörtern, verantwortlicher Umgang mit Drucksachen und ein maßgeschneidertes Paket an weiteren Sicherheitsmaßnahmen könnten bereits gegen eine Vielzahl von Angriffen oder auch vor Schäden durch unbeabsichtigte Fehler schützen, betont Franz Obermayer, unter anderem geprüfter Datenschutzbeauftragter und einer der handverlesenen IS-Beauftragten des Bundesamtes für Sicherheit in der Informationstechnik (BSI).

Selbst wenn man gegen hochprofessionelle Nachrichten- und Spionagedienste keine Chance habe, selbst mit dem Schutz vor ganz gewöhnlichen Internet-Kriminellen oder Hackern mit böswilligem Humor sei schon viel gesichert. – ede