# Cybercrime und der Faktor Mensch

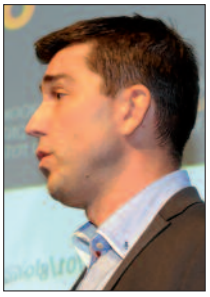
**Expertinnen und Experten aus der Polizei und der Privatwirtschaft beleuchteten bei einer Sicherheitskonferenz der Donau-Universität Krems die Rolle des Menschen in der Cyber-Kriminalität.**

In dem Spannungsfeld zwischen Unordnung und Möglichkeit liegen die Gefahren für die Menschen, die sich im Internet bewegen", sagte die Generaldirektorin für die öffentliche Sicherheit Dr. Michaela Kardeis bei der 16. Sicherheitskonferenz der Donau-Universität Krems zum Thema „Digitale Unordnung – Cybercrime und der Faktor Mensch" am 24. Oktober 2018. Täter im Cyber-Raum nutzen dieses Spannungsfeld aus. Die kriminellen Handlungen reichen von Erpressungen, Auskundschaften des Privatlebens, Betrügereien bis hin zu strafbarem Vorgehen rund um soziale Beziehungen. In einem Forschungsprojekt der Donau-Universität Krems, das von „KIRAS Sicherheitsforschung" gefördert wurde, wurden Fälle von Internetkriminalität in Wien aus den Jahren 2006 bis 2016 analysiert. Der Anteil der betroffenen Privatpersonen lag bei 38 Prozent, jener der Unternehmen bei 62 Prozent; das Durchschnittsalter bei knapp über 47 Jahren.

Laut Generaldirektorin Kardeis können Internetnutzerinnen und -nutzer selbst dazu beitragen, strafbare Handlungen zu verhindern, indem sie Angeboten im Internet eine gesunde Skepsis entgegenbringen. In vielen Fällen helfen Kontrollen und die Prüfung auf Plausibilität, wenn man etwa eine E-Mail über eine vermeintliche Notlage eines Bekannten oder die Nachricht einer plötzlichen Erbschaft eines bisher unbekannten Verwandten erhält.

Ratsam sei auch, sich beim Kauf von Geräten mit Internetverbindung für Produkte mit besseren Sicherheitsvorkehrungen zu entscheiden und für jeden Online-Dienst und jedes Gerät unterschiedliche, sichere Passwörter zu verwenden, die regelmäßig gewechselt werden. „Genauso wie Expertinnen und Experten braucht es zur Schaffung von digitaler Ordnung und somit mehr Sicherheit auch wissende Bürgerinnen und Bürger, die die Gefahren des Internets kennen und sich ihrer eigenen Möglichkeiten zum Schutz im Cyber-Raum bewusst sind. Damit ihnen das gelingt, brauchen sie Unterstützung und einen Schulterschluss der Behörden, der Wissenschaft, der Wirtschaft und der Gesellschaft", erläuterte Generaldirektorin Kardeis.

**Leopold Löschl: „Die klassische Kriminalität verlagert sich ins Internet."**



**Joe Pichlmayr: „Kriminelle setzen Social-Engineering-Techniken ein."**

**Boomender Markt.** Josef Pichlmayr, *IKARUS Security Software,* verwies auf eine Statistik des Sicherheitssoftware-Anbieters *Bromium,* die den Markt für Cybercrime mit 1,5 Billionen US-Dollar einschätzt (Stand April 2018). Ein Blick auf die größten Datendiebstähle der jüngsten Vergangenheit zeigt, in welchem Umfang sich diese Daten-Märkte entwickelten. Darunter drei Milliarden *Yahoo*-User-Profile, 150 Millionen Fitness/Ernährungsdaten von *UnderArmor,* 145 Millionen Kunden/Kaufdaten von *E-Bay,* 143 Millionen Datensätze bei *Equifax* über Verbrauchergebaren und Kreditwürdigkeit.

„Das Erpressungs-Segment veranschaulicht auf beeindruckende Weise, wie rasch Wertschöpfungsketten entstehen und sich weiterentwickeln", sagte Pichlmayr. Es habe wenige Jahre gedauert von den ersten Cryptoware-Trojanern, mit denen Daten auf Rechnern verschlüsselt wurden und für deren Freigabe Opfer zur Zahlung eines Lösegeldes erpresst wurden, bis zu Cryptomining-Bots, wo Rechner angezapft werden, um mit deren Hilfe Rechenleistung für die Erzeugung digitaler Währungen wie *Bitcoin* zu gewinnen.

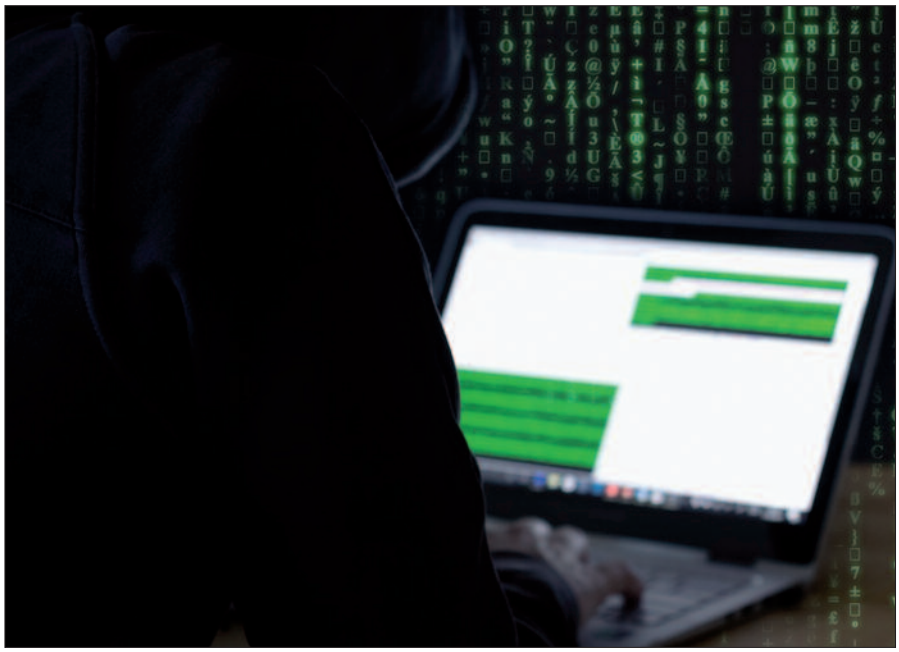
**Michaela Kardeis: „Internet-Angebote mit Skepsis betrachten."**

**Angriffe gegen kritische Infrastruktur und den Finanzsektor** zeigten, dass es keine geschützten Räume vor Cyber-Attacken gibt. Angriffe im Finanzsektor richteten sich anfangs gegen Kunden und deren Infrastruktur. Angriffe mit den Schadprogrammen „Carbanac" und „Corcow" zeigten, dass weder Geldausgabeautomaten, das „Swift"-Netzwerk, noch andere bankeninterne Zahlungsprozesse und Handelssysteme vor Währungstransaktions-Manipulationen oder direkten Geld-Transfers gefeit waren und sind. Statt via Online-Banking-Betrugs Tausende Opfer um ein paar Tausend Euro zu betrügen, verschafften sich Angreifer mit einem Angriffsframework namens „Anunak" Zugang zu über 50 russischen Banken und fünf Bezahlsystemen und stahlen rund 25 Millionen Dollar.

„Social Engineering", das Manipulieren von Menschen, zählt bei allen technischen Raffinessen zu den erfolgreichsten Komponenten für eine Vielzahl an Angriffen – gleich ob Nigeria-Scam, Vorschuss-Betrug, Up-front-Kosten für Gewinne, Phishing oder Spearphishing, Fake-Shops, betrügerische Anrufe, Abzocke via Schnäppchen bis zu ausgeklügelten CEO-Fraud-Angriffen. „Wenn Cyber-Kriminelle Social-Engineering-Techniken einsetzen, sind sie – von Ausnahmen abgesehen – meist ziemlich effizient", sagte Pichlmayr.

**Cyber-Sicherheitsvorfälle** abwehren. Ing. Thomas Mandl, *Cyber Defense Consulting Experts e.U.,* berichtete, wie Unternehmen auf Cyber-Bedrohungen reagieren, welche technischen und organisatorischen Schutzmaßnahmen sich in der Vergangenheit bewährt haben und warum der Faktor Mensch nach wie vor – trotz Awareness Schulungen – wichtiger denn je ist, um Cyber-Bedrohungen erfolgreich abwehren zu können. Vor allem kleinere und mittlere Unternehmen, wo IT-Security-Experten knapp sind – haben kaum eine Wahl und müssen sich verstärkt auf Schutz-

Fotos: Andrea Reischer/Donauuni Krems



**Cybercrime: Ein hohes technisches Know-how zur Begehung von Cyber-Delikten ist heute keine unbedingte Notwendigkeit mehr.**

technologie verlassen. Hersteller integrieren immer mehr Funktionalität in Produkte, obwohl diese nur ein Bruchteil der Anwender benötigt – nur, um neue Features „verkaufen" zu können. „Dadurch erhöht sich die Angriffsoberfläche auf diese Produkte, was wiederum in erhöhtem Schutzbedarf resultiert", sagte Mandl. Könnte man auf einer „grünen Wiese" beginnen, würde jeder IT-Security-Architekt ein aufeinander abgestimmtes Security-Portfolio bevorzugen.

„In der Praxis haben wir es aber mit einer, über die Jahre gewachsenen und heterogenen – oft nicht miteinander kompatiblen – IT-Security-Infrastruktur zu tun, die aus vielen Insellösungen besteht", erläuterte Mandl. Beispielsweise wird der Anti-Viren-Schutz von Hersteller A, mit einer Firewall von Hersteller B kombiniert und ein Angrifferkennungssystem von Hersteller C genutzt. „Die Lösungen alleine sind sicherlich gut, sie können aber nicht aufeinander abgestimmte Sicherheitslösungen in der komplexen Cyber-Welt und nicht den Mehrwert bringen, den ein Unternehmen eigentlich bräuchte", erklärte Mandl.

Eine laufende Überwachung der IT-Infrastruktur hinsichtlich Betriebsparameter wie z. B. Systemauslastung, Speicherverbrauch, Netzwerkbandbreitenverbrauch, Verfügbarkeit von Systemen/Services, etc. gehört bereits seit Langem zu den Grundbausteinen eines IT-Betriebs. Die Überwachung von Sicherheitsparametern durch ein *SIEM (Security Information Event Management System)* hält nur sehr zögerlich Einzug in den Unternehmen. „Dies liegt laut Aussagen einiger IT-Leiter und Geschäftsführer oft daran, dass die eigenen IT-Betriebsteams wenig Ahnung von IT- und Informationssicherheit haben und auch auf Grund von Ressourcenmangel mit der Aufrechterhaltung des IT-Betriebs ausgelastet sind", erklärte Mandl. Zusätzliche Security-Aufgaben seien nebenbei schwer zu bewältigen. Dabei könnte laut Mandl diese Technologie – wenn sie richtig eingesetzt wird, und man einen hohen Automatisierungsgrad erreichen kann – besonders bei der Früherkennung von Sicherheitsvorfällen helfen.

**Cyber-Ermittlungen.** Besonders aufseiten der Täter haben sich die Möglichkeiten zur Begehung von Cyber-Straftaten gewaltig erweitert. Mit der fortdauernden Vernetzung unserer Lebensbereiche und dem Ausbau der Datennetze steigt die Zahl der potenziellen Opfer an", sagte Mag. Leopold Löschl, Leiter des *Cybercrime-Competence-Centers (C4)* im Bundeskriminalamt. In diesem Spannungsbogen der Cybercrime-Ermittlungen spielt der „Faktor Mensch" die zentrale Rolle. Bereiche der „klassischen" Kriminalität verlagern sich mehr und mehr in den Cyber-Raum. Die Verfügbarkeit von geschützten Bereichen im Darknet, kriminellen Dienstleistern und Krypto-Währungen erleichtern diese Prozesse und fördern das Kriminellwerden auch von bisher nicht kriminellen Personen. Gleichzeitig eröffnen die anhaltende Vernetzung aller Lebensbereiche, das Internet der Dinge und der Einsatz von künstlicher Intelligenz laufend neue Angriffsflächen.

Während die Zahl herkömmlicher Kriminalitätsformen stagniert oder rückläufig ist, steigen die Deliktszahlen bei Cybercrime seit Jahren stetig an. In der Kriminalstatistik des Bundeskriminalamtes lag 2014 die Anzahl der angezeigten Fälle bei 8.966 – 2017, drei Jahre später, wurden mit 16.804 Anzeigen fast doppelt so viele Fälle gemeldet.

**Täter.** Ein hohes technisches Know-how zur Begehung von Cyber-Delikten ist heute keine unbedingte Notwendigkeit mehr. Fertige Tools, Anleitungen und Dienstleistungen, gepaart mit krimineller Energie, reichen, um zum Cyberkriminellen zu werden. „Der Glaube, nicht entdeckt zu werden sowie die meist fehlende Konfrontation mit den Opfern senken die Hemmschwelle zur Tatbegehung zusätzlich", sagte Löschl.

**Opfer.** Ist jemand Opfer geworden, sind Scham, Ängste oder Verzweiflung oft so groß, dass keine Anzeige erstattet wird. Bei Unternehmen ist es der vermeintliche Verlust an Reputation, der die Opfer hindert, Meldung bei der Polizei zu erstatten. Darüber hinaus trägt das mangelnde Vertrauen der Opfer in die Strafverfolgung zum hohen Dunkelfeld bei. Die eigene Gutgläubigkeit und das Vertrauen vieler Menschen in das Internet sind bei Opfern häufig anzutreffende Merkmale. Oft haben die Opfer keinen Bezug zur Technik und den grundlegenden Sicherheitsvorkehrungen, sie verstehen sich selbst nur als oberflächliche Nutzer. Der eigene Schutz persönlicher Daten wird aufgrund des offenen und transparenten Lifestyles kaum beachtet.

„Bei zahlreichen Cyber-Delikten spielt auch eine Nahebeziehung des Täters zum Opfer eine wichtige Rolle – wie zum Beispiel bei Cybermobbing oder Cyberstalking", erläuterte Löschl. Die Opfer werden über das Internet persönlich angegriffen, diffamiert und psychisch terrorisiert. Viele Betroffene fühlen sich hilflos diesen Attacken ausgeliefert und überdies vor nahezu jedermann bloßgestellt. „Die fortschreitende

FOTO: WEIXX - STOCK.ADOBE.COM

Vernetzung eröffnet dabei für die Täter noch zusätzliche Möglichkeiten“, sagte Löschl.

**Strafverfolgung.** Die klassische „analoge“ Ermittlungsarbeit der Polizei unterscheidet sich fundamental von IT-Ermittlungen und deren Möglichkeiten und Herausforderungen. „Ermittler im Cyber-Raum müssen neben dem allgemeinen kriminalpolizeilichen Handwerkszeug über technisches Wissen verfügen, um erfolgreich ermitteln zu können“, sagte Löschl. Kenntnisse über IP-Adressen, virtuelle Währungen, das Darknet und die Fähigkeit, E-Mail-Header oder Logfiles auszulesen sind ebenso erforderlich wie Ausbildungen in der forensischen Datensicherung und Netzwerkermittlung. Trotz aller technologischer Kenntnisse seien laut Löschl vor allem das polizeiliche Wissen und die kriminalistische Erfahrung ausschlaggebend für Ermittlungserfolge.

**Cyber-Sicherheit und Prävention.** „Oft herrscht das Bild vor, dass Cyber-Sicherheit eine Sache der Technik und der IT ist. Man darf aber trotz immer besserer technischer IT-Sicherheitslösungen nicht vergessen, dass der Faktor Mensch eine entscheidende Rolle bei der Aufrechterhaltung der Cyber-Sicherheit spielt“, sagte Dipl.-Ing. Philipp Blauensteiner, Leiter des Cyber-Security-Centers im Bundesamt für Verfassungsschutz und Terrorismusbekämpfung.

Auch bei großen Cyber-Angriffen, die die Daseinsvorsorge zahlreicher Menschen massiv beeinträchtigt haben, war oft das Überlisten eines Benutzers, der erste Schritt des Eindringens. Studien belegen, dass dies nicht nur Einzelfälle sind, sondern dass dies die Vorgehensweise bei der überwältigenden Anzahl der Cyber-Angriffe ist. „Eine wirksame Prävention kann nur dann funktionieren, wenn neben technischen Maßnahmen und organisatorischen Vorkehrungen die Bewusstseinsbildung bei jedem und jeder Einzelnen einbezogen wird“, sagte Blauensteiner.

**Phishing.** Die Firma *PhishMe* schätzt den Anteil an Cyber-Angriffen, deren erster Schritt durch einen Benutzer ermöglicht wird, der mit Hilfe eines Phishing-Mails überlistet wird, auf 91 Prozent. Laut eines Berichts der Firma *Dcoya* stand am Anfang von 80 Prozent der erfolgreichen Schadsoftware-Angriffe und 95 Prozent der erfolgreichen Spionage-Angriffe ein erfolgreicher Phishing-Versuch. Das heißt, in diesen Fällen wurde von einem Benutzer ein unsicherer Anhang geöffnet oder auf einen Link geklickt und dieser auf eine präparierte Webseite geleitet.


**Sicherheitskonferenz Krems: Martin Tandinger, Josef Edlinger, Thomas Ratka, Maresa Meissl, Walter Seböck, Michaela Kardeis, Rudolf Striedinger, Martin Jawurek.**

Auf dieser wird nun das Opfer aufgefordert, sensible Informationen (z. B. Passwörter) preiszugeben. Es kann sein, dass allein der Besuch dieser Seiten zu einer Infektion mit Schadsoftware führt, durch einen „Drive-by-Download“, der Schwachstellen im Browser ausnutzt. Beim Spear-Phising wird von den Angreifern mehr Energie für die Vorbereitung und Durchführung der Angriffe investiert, sodass die entsprechende Mail auf das Opfer maßgeschneidert werden kann.

Am Beginn einer Vielzahl großer Angriffe standen Spear-Phishing-Mails. Am Anfang des Spionage-Angriffs auf den deutschen Bundestag stand eine am 30. April 2015 an mehrere Bundestagsabgeordnete versandte, gefälschte E-Mail, die vorgab, von einem Mailserver der Vereinten Nationen zu kommen. Darin enthalten war ein Link zu einem vermeintlichen UN News-Bulletin. Wer auf diesen Link klickte, wurde zu einer manipulierten Webseite geleitet, die einen Drive-by-Download auslöste.

**Philipp Blauensteiner: „Der Mensch spielt eine entscheidende Rolle bei der Aufrechterhaltung der Cyber-Sicherheit.“**

Da Angreifer auf Technik und auf Social Engineering, also das Ausnutzen der „Schnittstelle Mensch“ setzen, ist es notwendig, in der Verteidigungsstrategie auf technische Hilfsmittel sowie auf organisatorische Maßnahmen und auf die Absicherung des „Faktors Mensch“ zu setzen. Vordringliches „Ziel muss sein, das Bewusstsein eines jeden Einzelnen im Bereich Cyber-Sicherheit zu heben. Wichtig ist auch zu vermitteln, dass Sicherheit kein Zustand ist, den man einmal erreicht und dann hält. Sicherheit ist vielmehr ein Prozess, der permanent gelebt und weiterentwickelt werden muss“, sagte Blauensteiner.

Einen weiteren Vortrag gab es zu den Themen „Schwachstellen finden. ERP Security in der Praxis“, von Dipl.-Ing. Mag. Andreas Tomek und Mag. Severin Winkler, *KPMG Security Services*.

**Tagungsband.** Die Vorträge der 16. Sicherheitskonferenz wurden in einem Tagungsband publiziert. Er steht als E-Book zur Verfügung unter: *www.donau-uni.ac.at/sicherheitskonferenz*.

Studienangebote der Donauuniversität Krems: *www.donau-uni.ac.at/de/index.php*

Fotos: Andrea Reischer/Donauuni Krems