Geld und Rache

Cybercrime war das zentrale Thema des von Bundesministerium für Inneres und der Opferschutzeinrichtung WEISSER RING veranstalteten Tags der Kriminalitätsopfer.

Das wachsende Phänomen Cybercrime stellt sowohl die Exekutive als auch Opferhilfe-Einrichtungen vor neue Herausforderungen. Während die Statistik in fast allen Bereichen der Kriminalität rückläufig ist bzw. gleich bleibt, lassen sich bei Internet-Kriminalität seit Jahren steigende Zahlen beobachten – sowohl wenn es um Straftaten geht, die Informations- und Kommunikationstechnik nutzen, als auch um solche, durch die Informations- und Kommunikationstechnik vorsätzlich manipuliert und geschädigt wird. Deshalb stellten Bundesministerium für Inneres und WEISSER RING Verbrechensopferhilfe das Thema Cybercrime ins Zentrum des diesjährigen Tags der Kriminalitätsopfer am 22. Februar 2019.

Tag der Kriminalitätsopfer im Innenministerium: Dina Nachbaur, Udo Jesionek, Karoline Edtstadler, Bernadett Humer, Peter Goldgruber, Michael Lepuschitz.

Täterprofile und typische Tathergänge. Die voranschreitende Digitalisierung führt dazu, dass Internetkriminalität mittlerweile fast jeden treffen kann. Firmen, Staaten oder Privatpersonen können Opfer werden. Der Bogen spannt sich von Hacking-Delikten bis hin zu Cyberstalking.

Seit 2006 werden in Österreich die Fälle von Computerkriminalität in der amtlichen Kriminalstatistik unter dem Sammelbegriff „Cybercrime“ erfasst. Dr.in Edith Huber, Sicherheitsforscherin und Leiterin der Stabsstelle Forschungsservice und Internationales an der Donau-Universität Krems, stellte unter dem Titel „Täterprofile und typische Tathergänge“ die Ergebnisse eines von KIRAS geförderten Forschungsprojekts vor. Von 2006 bis 2016 wurden 5.404 Akten des Wiener Straflandesgerichts wissenschaftlich untersucht und es wurde zwei zentralen Fragen nachgegangen:

- Wie sehen typische Profile der Cyber-Kriminellen in Österreich aus?
- Lassen sich bestimmte Muster im Tathergang erkennen?

Dabei zeichneten sich zwei Tendenzen ab: Einerseits steigt die Zahl der Delikte, hinter denen finanzielles Interesse steht, wie beispielsweise der Identitätsdiebstahl. Andererseits wächst auch die Zahl der Delikte, die durch Rache motiviert sind.

Eine weitere wesentliche Erkenntnis ist, dass Täter nicht für jede Straftat, die im Internet begangen wird, überdurchschnittliche EDV-Kenntnisse brauchen. Es kann davon ausgegangen werden, dass rund zwei Drittel über ein geringes Bildungsniveau sowie maximal über Grundkenntnisse im Umgang mit EDV verfügen. Sie begehen einfache Delikte und verlagern die Kleinkriminalität aus der analogen in die digitale Welt. Auch Stalking findet zunehmend im Internet statt.

Robert Lakits, Bernhard Jungwirth: Vortragende am Tag der Kriminalitätsopfer.

Passwörter schützen. Daraus leitet sich auch eine zentrale Empfehlung der Wissenschafterin an alle Internet-Nutzerinnen und -nutzer ab: „Schützen Sie Ihre Passwörter auch vor Menschen, die Ihnen nahestehen.“ Denn das Wissen über die Passwörter Nahestehender eröffnet beispielsweise nach einer Trennung ungeahnte Möglichkeiten zur Rache. Immer wieder kommt es vor, dass ein gekränkter Ex-Partner die Passwörter von E-Mail und sozialen Medien ändert und damit für die eigentliche Besitzerin den Zugriff auf die Konten unmöglich macht oder sogar im Namen der betroffenen Frau intime Fotos versendet und persönliche Daten von ihr ins Internet stellt. Von den Delikten, die zur Anklage kommen, handelt es sich bei 43 Prozent um Rachedelikte. Die zweitgrößte Gruppe betrifft mit 29 Prozent Finanzdelikte.

Bei den Finanzdelikten setzt die Watchlist Internet *(www.watchlist-internet.at)* an. Der *Internet-Ombudsmann* informiert hier mit Unterstützung von *Netidee,* Bundeskriminalamt und *Willhaben* über aktuelle Betrugsfallen im Netz. Ing. Mag. Bernhard Jungwirth, M.Ed., Geschäftsführer *ÖIAT* und Leiter *Internet-Ombudsmann* setzt auf Prävention: Ziel der *Watchlist Internet* ist es, Internetnutzerinnen und -nutzer in der Sekunde des Zweifels zu erreichen – also genau in dem Moment, in dem sie sich Fragen stellen wie beispielsweise: Handelt es sich bei diesen günstigen Angeboten um einen Fake-Shop? Ist die Aufforderung zur Passwort-Änderung wirklich von meiner Bank? Kann der Absender der Nachricht tatsächlich eine intime Videoaufnahme von mir besitzen? Viele Menschen suchen in einer derartigen Situa-

Fotos: Gerd Pachauer, Orhan Maglajlić

tion mit Hilfe von *Google* & Co nach weiteren Informationen. Dafür stellt *Watchlist Internet* suchmaschinen-optimierte, niederschwellig aufbereitete Warnmeldungen bereit und beantwortet drei Fragen:

- Handelt es sich in einem konkreten Fall um Betrug?
- Was kann ich tun, wenn ich in eine Betrugsfalle geraten bin?
- Wie kann ich mich vor Internet-Betrug schützen?

Die Warnungen der *Watchlist Internet* erreichen inzwischen mehr als 100.000 Personen pro Monat.

Deep Web und Darknet. Chefinspektor Robert Lakits, Bundeskriminalamt, entführte die Zuhörerinnen und Zuhörer ins Deep Web und Darknet – jene 96 Prozent des Angebots im Internet, die sich außerhalb des Zugriffs von Suchmaschinen befinden. *Deep Web* und *Darknet* bieten Anonymität.

Für die Nutzung dieser Anonymität gibt es zwei Hauptmotive. Einerseits geht es um die Möglichkeit, auf Inhalte zuzugreifen, die im *Clear Web* (Internet) zensiert oder politischen Restriktionen unterworfen sind. Menschen, die den Schutz des *Deep Webs* für ihre Kommunikation benötigen wie beispielsweise Journalistinnen und Journalisten, schützen hier ihre Informanten und Quellen. Dissidentinnen und Dissidenten, Oppositionelle aus Diktaturen aber auch Whistleblower teilen sensible Daten und Informationen. Es geht um den Schutz vor den negativen Folgen ihrer Aktivitäten und vor staatlicher Verfolgung.

Auch die zweite Gruppe nutzt die Anonymität des *Deep Webs,* um sich der Strafverfolgung zu entziehen. Dabei handelt es sich um Personen, deren Handeln – sollte es im Internet gesetzt werden – sofort zu Anzeigen und strafrechtlicher Verfolgung führen würde. Im *Darknet* finden sich Foren, in denen sich Pädophile austauschen oder Tauschbörsen, auf denen kinderpornografisches Material, Videos von Morden und Misshandlungen, geteilt werden.

In Webshops und auf Handelsplattformen werden Waren und Dienstleistungen angeboten die verboten, reglementiert, illegal oder Restriktionen unterworfen sind. Der Bogen spannt sich vom Waffenhandel über geschützte Tiere oder Diamanten bis zu Dienstleistungen wie der Suche nach einem „Hitman“ für die Beseitigung ungeliebter Zeitgenossen. Klar ist, dass Cyber-Kriminelle kein Recht auf Nutzung der Anonymität bei ihren kriminellen Geschäften haben. Leider hat die Einführung von Kryptowährungen das Darknet aber gerade auf dem Gebiet der unerlaubten Geschäfte befeuert.

Die Arbeit des *Cybercrime-Competence-Centers* im Bundeskriminalamt, neue Fahndungmethoden und eine bessere Vernetzung der Polizei steigern den Fahndungsdruck im Darknet.

Weitere Vorträge und Grußadressen rundeten die ausgesprochen informative und vielfältige Veranstaltung ab. Assoz. Prof.in Mag.a Dr.in Ulrike Zartler, PD, Institut für Soziologie der Universität Wien, präsentierte eine brandneue im Rahmen des Projekts „Zivilcourage 2.0“ erstellte Studie zum Verhalten jugendlicher Online-Bystander. Erste Ergebnisse zeigen, dass sich Online-Zivilcourage aus Sicht von Jugendlichen stark von Offline-Zivilcourage unterscheidet: während im Alltagsverständnis Assoziationen wie „Mut“ und „Hel-

WEISSER RING

Ehrenamtliche vor den Vorhang

Unter den Menschen, die im Lauf der vergangenen 40 Jahre ihre Freizeit für die Anliegen des WEISSEN RINGS zur Verfügung gestellt haben, sind zahlreiche Mitarbeiterinnen und Mitarbeiter der Exekutive. Am Tag der Kriminalitätsopfer 2019 bedankte sich Innenminister Herbert Kickl in festlichem Rahmen bei 34 von ihnen für diesen Einsatz.

„Ich möchte Ihnen meinen Respekt und meine Anerkennung aussprechen für das, was Sie alle im Rahmen Ihrer ehrenamtlichen Arbeit beim WEISSEN RING leisten,“ betonte der Innenminister bei seiner Ansprache im Festsaal des Ministeriums. Er hob das große private Engagement hervor, das hinter diesem Einsatz von Freizeit steckt und wies darauf hin, dass die Tätigkeit als Exekutivbediensteter und die ehrenamtliche Arbeit für Verbrechensopfer beide in demselben Geist der Menschlichkeit und Nächstenliebe erfolgen. „Es ist mir eine große Freude zu wissen, dass die Exekutive hier einen wichtigen Beitrag leistet.“ Jedes Verbrechen stelle einen Einschnitt im Leben dar – nach diesem Tag ist alles anders. Da brauche es Empathie und die Bereitschaft und Fähigkeit zuzuhören. „Ich danke Ihnen ganz persönlich und im Namen der Republik Österreich für Ihre Tätigkeit in diesem so schwierigen und wichtigen Bereich.“

Kickl würdigte auch Prof. Dr. Udo Jesionek, Präsident des WEISSEN RINGS, für die beeindruckende Energie, mit der er das „Projekt WEISSER RING“ weitertreibe und attestierte dem Verein eine Erfolgsbilanz jenseits von dem, was in Zahlen messbar ist.

Foto: Gerd Pachauer

Edith Huber: „Passwörter auch vor Menschen schützen, die einem nahestehen."

dentum" mit Zivilcourage verknüpft sind, werden Online Interventionen nicht als besonders couragiert betrachtet. Geschäftsführerin Dr.in Dina Nachbaur und Mag.a Sabine Weber, beide WEISSER RING, präsentierten unter dem Titel „Gemüsehass und Identitätstorte" alternative Trainingsmethoden für die Weiterbildung von Mitarbeiterinnen und Mitarbeitern in Opferhilfe-Einrichtungen, die sich in mittlerweile 20 Trainings bewährt haben. Die Schulungsunterlagen wurden im Rahmen des Projekts „Combatting gender-based cyber-violence" vom WEISSEN RING gemeinsam mit dem Forschungszentrum Menschenrechte der Universität Wien erstellt und können beim WEISSEN RING angefordert werden.

Generalsekretär Mag. Peter Goldgruber, der die Veranstaltung in Vertretung von Innenminister Herbert Kickl eröffnete, plädierte für einen entsprechenden Umgangston im Netz: „Allen soll bewusst sein, dass die Worte, die man sagt oder schreibt, auch Wirkung zeigen."

Staatssekretärin Mag.a Karoline Edtstadler bekräftigte, dass es nicht möglich sein wird, mit den Methoden von gestern jene Verbrechen zu bekämpfen, die heute schon mit den Methoden von morgen verübt werden. Und sie stellte klar, dass auch Straftaten, die im digitalen Raum verübt werden, bei den Betroffenen ganz reale Spuren hinterlassen.

Bernadett Humer, MSc, Kabinettschefin der Bundesministerin für Frauen, Familie und Jugend, betonte: „Es ist wichtig, junge Menschen darin zu bestärken, sich Hilfe zu holen" und verwies auf diesbezügliche Anlaufstellen wie die Familienberatungsstellen.

Hon. Prof. Dr. Udo Jesionek, Präsident des WEISSEN RINGS, bedankte sich beim Bundesministerium für Inneres für die erfolgreiche Zusammenarbeit und verlieh der Hoffnung Ausdruck, dass auch dieses Symposium – wie bereits in den Jahren zuvor – die Zusammenarbeit zwischen den Beteiligten und allen am Thema Interessierten weiter verbessern wird. *B. P.*

FOTO: ORHAN MAGLAJLIĆ