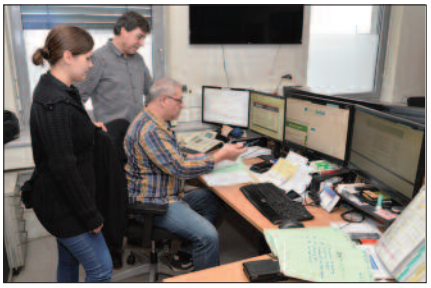
Weniger Anzeigen

Das Bundeskriminalamt verzeichnete 2014 zwar weniger Anzeigen bei Cybercrime-Delikten. Im Zehn-Jahresvergleich ist aber ein deutlicher Trend nach oben erkennbar.

Die Zahl der Anzeigen wegen Cybercrime sank von 10.051 Anzeigen (2013) um elf Prozent auf 8.966 (2014). Die Zahl der Internetbetrugsdelikte sank um 13,5 Prozent von 7.667 (2013) auf 6.635 (2014). Zurückgegangen ist auch die Zahl der Anzeigen wegen § 126b Strafgesetzbuch (Störung der Funktionsfähigkeit eines Computersystems) – von 470 (2013) auf 118 (2014). Gestiegen ist die Zahl der Anzeigen wegen § 118a StGB (Widerrechtlicher Zugriff auf ein Computersystem) von 391 (2013) auf 677 (2014). Die Aufklärungsquote lag 2014 bei 40,8 Prozent, um 4,4 unter der Zahl von 2013. Dieser Rückgang ist laut Bundeskriminalamt unter anderem auf die immer stärkere Professionalisierung der international vernetzten Tätergruppen zurückzuführen.

Auch wenn es 2014 einen Rückgang der Cyber-Kriminalität gab, ist im Zehn-Jahresvergleich ein deutlicher Trend nach oben erkennbar. Dies ist durch die zunehmende Verbreitung von Computern zu erklären – speziell in Form von Smartphones und Tablets – und des Ausbaus von Netzwerken, vor allem mobiler Breitbandverbindungen. Zu den häufigsten Cybercrime-Vorfällen 2014 zählten „falsche Microsoft-Mitarbeiter“, Erpressung mittels Ransomware, Abzocke durch Notfall-E-Mails und Betrügereien auf Verkaufsplattformen.

Falsche Microsoft-Mitarbeiter. Kriminelle geben sich am Telefon als *Microsoft*-Mitarbeiter aus und sagen dem Kunden, dass sein Computer mit Schadsoftware infiziert sei. Dadurch sei *Microsoft* auf den Kunden aufmerksam geworden. Der vermeintliche Mitarbeiter bietet an, die Schadware vom Computer des Kunden kostenlos zu entfernen. Damit er sich mit dem Gerät des Kunden verbinden könne, wird dieser aufgefordert, ein „Remote-Zugriffstool“ für Fernwartungen – zum Beispiel „Team Viewer“ – herunterzuladen und zu installieren. Nach Installation der Software und Bekanntgabe eines Zugriffscodes für das Remote-Tool kann der angebliche *Microsoft*-Mitarbeiter auf die Daten des Computers zugreifen. Während der „Bereinigung“ des Systems lenkt der „Microsoft-Mitarbeiter“ den Kunden durch unwichtige Erklärungen ab. Dazwischen bleibt der Bildschirm schwarz, wodurch für den Kunden nicht ersichtlich ist, nach welchen Daten der Kriminelle auf der Festplatte sucht. Nach „Bereinigung des Systems“ oder nachdem der Täter Daten zu sich übertragen hat, wird darauf verwiesen, dass eine Lizenz abgelaufen sei und günstig verlängert werden könne. Die angebotene Lizenz zum Preis von zehn bis 30 Euro für den weiteren Schutz des Systems soll dann vom Kunden sofort bezahlt werden. Dafür wird ein Formular zur Verfügung gestellt. In den meisten Fällen bittet der „Microsoft-Mitarbeiter“ den Kunden, die Bezahlung durch die Eingabe von Kreditkartendaten oder mit Online-Banking zu erledigen, um seine Bankdaten auszuspähen.



Cybercrime-Meldestelle im BK: Der Schwerpunkt der Anfragen lag 2014 bei Phishing- und Spam-Mails.

Ransomware. Kriminelle verschlüsseln Daten auf dem Computer und verlangen für die Entschlüsselung ein „Lösegeld“. 2014 wurden in Tirol zahlreiche Ransomware-Fälle bekannt. Betroffen waren neben Privatpersonen auch einige kleinere Unternehmen. Die Zahl der betroffenen Computer dürfte laut den Cybercrime-Ermittlern weitaus höher liegen, da nur ein Bruchteil der betroffenen Personen bzw. Firmen Anzeigen erstatte. Die Erpresser-Software wird meist als manipulierte E-Mail-Anhänge getarnt bzw. mit präparierten Webseiten auf den Computer des Besuchers installiert – während des Betrachtens einer Webseite (Drive-By-Download). Anschließend durchsuchen die Kriminellen das infizierte System inklusive der externen Datenträger und Netzwerkfreigaben und verschlüsseln Dateien. Die neueren Versionen dieser Schadsoftware verwenden meist zwei Verschlüsselungsdurchläufe mit langen, zufälligen Passwörtern und löschen danach die ursprünglichen Dateien mit Löschprogrammen, sodass ein Wiederherstellen auch für professionelle Datenretter unmöglich wird. Abschließend werden auf den befallenen Computern Startseiten installiert, in denen auf die Verschlüsselung und Löschung der Daten hingewiesen wird.

Die Täter bieten an, die Verschlüsselung durch Zahlung eines Geldbetrags über verschlüsselte Kanäle aufzuheben. Die Schäden für die betroffenen Privatpersonen bzw. Unternehmen sind hoch. Nicht mehr vorhandene Kundendaten, fehlender Schriftverkehr und gelöschte Buchhaltung usw. können die Betroffenen an den Rand einer Insolvenz bringen. Neben den allgemeinen Sicherheitshinweisen zum Verhalten im Internet hilft ein ständiges Backup auf externe bzw. abgekoppelte Systeme.

„Notfall-E-Mails“. Bei diesem Cyber-Angriff werden E-Mail-Accounts durch Hacking- oder Phishing-Attacken übernommen. Absicht der Täter ist es, an die Daten des E-Mail-Adressbuches ihrer Opfer zu gelangen und an diese Kontakte eine „Notfall-E-Mail“ zu senden. Darin geben sie an, dass ihnen im Urlaub oder auf einer Auslandsreise Geld und/oder Dokumente gestohlen wurden und bitten um Überweisung von Geld, um die offene Hotel- oder Flugrechnung zu bezahlen, da ihnen sonst eine Heimreise nicht möglich ist. Sie würden das geborgte Geld sofort nach ihrer Rückkehr zurückgeben.

Die Überweisung soll meist über einen vom Täter vorgeschlagenen Money-Transfer-Dienst erfolgen. Hier ist eine Rückverfolgung des Geldflusses nahezu unmöglich. In den meisten Fällen werden die Passwörter der übernommenen E-Mail-Accounts vom Täter geändert, dass kein Zugriff mehr

FOTO: EGON WEISSHEIMER

durch den eigentlich Berechtigten erfolgen kann. Danach werden die Kontaktdaten gelöscht und es wird ein weiterer E-Mail-Account bei einem anderen Dienstanbieter erstellt. Der weitere E-Mail-Verkehr zwischen den Opfern und dem Täter findet nun über die neue E-Mail-Adresse statt, die alte Adresse dient zum Teil nur noch als Relay-Station.

Verkaufsplattformen. Im Juli 2014 zeigte ein österreichisches Unternehmen an, dass sein Online-Bezahlsystem gehackt und eingehende Beträge auf ein Konto der Täter umgeleitet worden seien. Mehrere Verdächtige wurden ausgeforscht, zwei konnten festgenommen werden. Von den Verdächtigen wurden nicht nur Webseiten gehackt, sondern auch Internetbetrugsdelikte begangen. Die Hacker gingen arbeitsteilig vor: Das Anbieten der Waren auf der Plattform *willhaben.at* erledigte ein Team, während die Kontoöffnung bzw. das Abheben der Geldbeträge eine andere Gruppe übernahm. Das erbeutete Geld wurde über verschiedene Internetdienste aufgeteilt.

Die Tätergruppen kannten sich nicht persönlich und die Kommunikation erfolgte via Chat im Internet. Bei der Auswertung der sichergestellten Datenträger wurde festgestellt, dass die Verdächtigen von einer Vielzahl von Geschädigten auch die Bank- und Kreditkartendaten mittels Phishing erlangten und mit diesen Daten Waren von Online-Shops zum Weiterverkauf bestellt worden waren.

Cybercrime-Bekämpfung. Das im Bundeskriminalamt angesiedelte Cybercrime-Competence-Center (C4) ist die Zentralstelle zur Bekämpfung von Cyber-Kriminalität in Österreich. Sie setzt sich zusammen aus den Bereichen zentrale Aufgaben, IT-Beweissicherung, Ermittlungen und der Meldestelle. Techniker des C4 leisteten 2014 in 15 Fällen Assistenz, für die technisches Spezialwissen erforderlich war. In der IT-Beweissicherung wurden 2014 in mehr als sechs Sonderkommissionen über 120 Terabyte an elektronischen Beweisen gesichert.

Mitarbeiter des Fachbereichs mobile Forensik werteten 1.200 mobile Geräte aus. Im Referat Ermittlungen werden auch Fälle wie die Schadsoftware *BlackShades,* Polizeitrojaner, Telefon-Phreaking usw. bearbeitet. *Blackshades* ist eine Schadsoftware, die es Nutzern ermöglicht, aus der Ferne Kontrolle über einen fremden Computer zu erlangen. Tastatureingaben lassen sich mitlesen, Screenshots anfertigen oder die Webcam bedienen, um etwa unbemerkt Bilder von ahnungslosen Opfern zu machen. Der Polizeitrojaner ist einer Form von Ransomware.

Falsche Webshops: Die Zahl der angezeigten Internetbetrugsdelikte sank um 13,5 Prozent von 7.667 (2013) auf 6.635 (2014).

Als Phreaking bezeichnet man das Hacken von Telefonsystemen, um kostenlos telefonieren zu können. „Phreaking“ ist eine Kombination aus „Phone“ und „Freak“.

Neben dem C4 auf Bundesebene bestehen in allen Landeskriminalämtern mit dem Assistenzbereich 06 (IT-Beweissicherung) dem C4 vergleichbare Dienststellen. In diesen Organisationseinheiten sind kriminalpolizeilich und technisch ausgebildete Experten mit der Bekämpfung von Cybercrime und der IT-Forensik in den jeweiligen Bundesländern befasst. Für die Bekämpfung von Cybercrime auf lokaler Ebene und zur Unterstützung der Kollegen in den Polizeiinspektionen wurden in den letzten Jahren rund 280 Bezirks-IT-Ermittler ausgebildet. Im Oktober 2014 wurde vom C4 erstmals eine Fachtagung für IT-Forensiker und Bezirks-IT- Ermittler organisiert.

Die Cybercrime-Meldestelle im Bundeskriminalamt *(against-cybercrime@bmi.gv.at)* bearbeitete im Jahr 2014 über 10.000 Mitteilungen von Bürgern sowie von in- und ausländischen Dienststellen. Der Schwerpunkt der Anfragen lag bei Phishing- und Spam-Mails. Eine Steigerung gab es bei Meldungen über versuchte Betrugsfälle auf Online-Plattformen, bei Ein- und Verkäufen im Internet – zumeist bei Kfz- oder Immobilienangeboten.

Die Mitarbeiter der Meldestelle hatten 2014 vermehrt mit Meldungen über Fake-Webshops und B2B-Shops und damit zusammenhängenden Betrugs- und Urheberrechtsverletzungen zu tun, Fällen von angeblichen „Microsoft-Mitarbeitern“, der Verständigung von über 40.000 in Österreich betroffenen E-Mail-Accounts nach einem in Deutschland vorgefallenen Datendiebstahl sowie mit Fällen von Ransomware wie *Crypto-Wall* und *Crypto-Locker*.

Es wurde Unterstützung für andere Dienststellen geleistet, wie zum Beispiel bei der Ausforschung von IP-Adressen im Falle von Selbsttötungsankündigungen, Gewaltvideos im Internet, die Verständigung von Betroffenen bei inkriminierten Webseiten und Domänen und mehr.

In dringenden Fällen kann über den C4-Journaldienst die Einleitung von Maßnahmen zur technischen Unterstützung anderer Dienststellen, Datensicherung, Handy- und Navigationssystemauswertung veranlasst werden, beispielswiese bei Selbsttötungsankündigungen im Internet. Experten des Bundeskriminalamts beteiligen sich an Veranstaltungen des *Kuratoriums Sicheres Österreich (KSÖ)* und der *Wirtschaftskammer Österreich* und unterstützen Initiativen wie *SaferInternet*

FOTO: EGON WEISSHEIMER

und den *Internetombudsmann,* um das Bewusstsein für die Gefahren zu schärfen, die mit der Verwendung des Internets und der sozialen Medien verbunden sind.

Die Abteilung Wirtschaftskriminalität im BK führte 2014 die Zusammenarbeit im Projekt „Unternehmen Sicherheit“ zwischen der *Wirtschaftskammer Österreich (WKO)* und dem BMI fort. Dabei informiert die *WKO* ihre Mitglieder über Betrugsarten im Internet auf Basis der Information durch das Bundeskriminalamt. Eine weitere Kooperation besteht mit dem „Österreichischen Institut für angewandte Telekommunikation“ (ÖIAT), das die Plattformen „Internetombudsmann“ und „Watchlist Internet“ betreibt. Darüber hinaus referieren BK-Experten in Fachvorträgen, Diskussionen und auf Kongressen über die Gefahren im Internet.

Im Kiras-Projekt „Social Media Crime“ wurde eine Analyse einschlägiger Kriminalitätsphänomene erstellt, die Aufschluss über Erscheinungsformen und über Ursachen und Folgen sowie Opfer- und Tätercharakteristika gibt. Die Ergebnisse wurden nach kriminalpolizeilichen Anforderungen strukturiert und kategorisiert. Anhand dieser Einteilung werden Präventions- und Gegenmaßnahmen aufgezeigt, die international eingesetzt wurden oder angedacht sind. Aufbauend auf diesen Erkenntnissen, wurden Handlungsempfehlungen entwickelt, die kriminalpolizeiliches Vorgehen dabei unterstützen sollen, „Social-Media-Crime“ langfristig zu reduzieren. Projektpartner waren die *SYNYO GmbH,* das *Austrian Center for Law Enforcement Studies (ALES)* der Universität Wien und das *Cybercrime-Competence-Center*.

Beratung. Bei Fragen zum Thema Computerkriminalität kann man sich an eine der Kriminalpräventionsstellen in ganz Österreich wenden. Diese sind kostenlos unter der Telefonnummer 059-133 erreichbar. Auf der Webseite und auf den Social-Media-Seiten des Bundeskriminalamts gibt die Polizei Tipps, wie man sich und seinen Computer im Internet schützen kann und informiert über Gefahren und Schutzmaßnahmen:

www.bundeskriminalamt.at
www.facebook.com/bundeskriminalamt