„Kompetenzen bündeln“

Carsten Meywirth, der Leiter der Abteilung „Cybercrime“ im deutschen Bundeskriminalamt, über aktuelle und künftige Herausforderungen im Kampf gegen Cybercrime.

Wie hat sich Cybercrime in den letzten Jahren entwickelt?

Die Anzahl der Cybercrime-Angriffe steigt, speziell im Bereich DDoS und Ransomware. Kriminelle Delikte verlagern sich immer stärker von der analogen in die digitale Welt. Wir unterscheiden bei Cybercrime grundsätzlich zwei Bereiche: Computerkriminalität im engeren und weiteren Sinn. Letztere umfasst Straftaten, bei denen die Täter das Internet als Tatmittel nutzen – sprich: Verbrechen mit internetverbundenen Strukturen durchführen. Davon zu unterscheiden sind Cybercrime-Delikte im engeren Sinn, die sich beispielsweise mit DDoS- und Ransomware-Attacken direkt gegen Netzwerke und Daten richten. Darauf liegt auch der Ermittlungsfokus meiner Abteilung. Die einzige Durchbrechung ist, dass wir auch gegen Betreiber und Administratoren illegaler Marktplätze im Internet und im Darknet ermitteln. Originär beschäftigt sich die Abteilung Cybercrime des Bundeskriminalamts in Deutschland mit Cyber-Angriffen auf kritische Infrastruktur sowie Bundesbehörden und deren Einrichtungen – und deren Zahl nimmt zu.

Wie hat sich die Bedrohungslage im Bereich Cybercrime durch die Corona-Krise verändert? Welche neuen Phänomene sind entstanden?

Die Corona-Krise war ein Brandbeschleuniger für Cybercrime-Delikte. Kriminelle Cyber-Akteure haben die damit verbundenen gesellschaftlichen Veränderungen rasch erkannt und zu ihren Gunsten ausgenutzt. So waren beispielsweise vor der Corona-Pandemie die meisten Arbeitsplätze physisch in einem Unternehmen angesiedelt. Nun musste quasi über Nacht auf Remote-Arbeit und Homeoffice umgestellt werden. Die gesamte Technik der Unternehmen war darauf ausgelegt, die Daten in Netzen der Arbeitsumgebung zu belassen und nicht die Kommunikation über internetgestützte Infrastruktur zu führen. Kriminelle Cyber-Akteure haben schnell die Schwachstellen bei den Zugriffsmöglichkeiten von außen auf das System erkannt und für sich genutzt. Darüber hinaus haben sie sich der Narrative, die die Pandemie geliefert hat, bedient. Beispielsweise, indem man sich als Mitarbeiter eines Gesundheitsamts ausgibt, um Daten zu erfragen.

Carsten Meywirth: „In Deutschland beschäftigen wir uns derzeit mit Cyber-Angriffen auf kritische Infrastruktur sowie Bundesbehörden und deren Einrichtungen.“

Nicht nur Cyber-Kriminelle agieren global auch die Ermittlungsbehörden. Wie wichtig ist die internationale Vernetzung der Sicherheitsdienste?

Sehr. Über die Jahre hinweg haben sich sicherheitsbehördliche Partnerschaften rund um den Globus entwickelt. In Europa ist Europol mit der „Joint Cybercrime Action Taskforce“ eine wichtige Plattform, auf der neueste Erkenntnisse ausgetauscht und aktuelle Bedrohungslagen besprochen werden. Solche Allianzen sorgen dafür, dass Ermittlungen gegen kriminelle Akteure in den jeweiligen Mitgliedstaaten nicht doppelgleisig geführt werden. Auf internationaler Ebene spielen die USA eine wichtige Rolle, die gemeinsam mit den anderen Mitgliedern der „Five Eyes“ (Anm. Vereinigtes Königreich, Kanada, Australien und Neuseeland) bei der Bekämpfung von Cybercrime weltweit führend sind.

Bei sehr großen Fällen wie der Zerschlagung des internationalen Cybercrime-Netzwerks „Emotet“ haben sich alle Player im Vorfeld mehrmals getroffen, um Erkenntnisse auszutauschen und sich zu koordinieren. Nur so konnten wir die einzelnen Puzzleteile der verschiedenen Ermittlungsbehörden zusammensetzen und das Netzwerk zerstören. Grundsätzlich liegt der Fokus unserer Ermittlungen immer auf zwei Bereichen: Der Überführung der Täter und der Zerschlagung der technischen Infrastruktur, mit der Verbrechen begangen werden.

Foto: Katharina Schiffl

Wie ist die Abteilung „Cybercrime“ organisatorisch im Bundeskriminalamt eingebettet?

Bis 2020 haben wir das Phänomen innerhalb der Abteilung „schwere und organisierte Kriminalität“ bearbeitet. Seit gut drei Jahren gibt es im Bundeskriminalamt die Abteilung Cybercrime als eine von elf Abteilungen. Bei uns werden verschiedene Kompetenzen gebündelt, um möglichst effektiv und schlagkräftig gegen Internetkriminelle vorzugehen: Kriminalbeamte, Analysten und IT-Experten mit unterschiedlichsten Spezialisierungen arbeiten Hand in Hand.

Wie schwierig ist es derzeit, IT-Experten zu rekrutieren – Stichwort: Fachkräftemangel?

Wir können zwar nicht mit jedem Gehaltsangebot aus der Privatwirtschaft mithalten, aber wir bieten ein attraktives Gesamtpaket. Gerade in der Cybercrime-Bekämpfung gewinnen wir auch mit dem großen Gestaltungspotenzial viele kreative und kluge Köpfe. Neben Kriminalisten bauen wir auch das technologische Know-how stark aus, etwa für Zugriffe auf Server, die Verfolgung von Identitäten im Darknet, oder auch die Ermittlung von Zahlungsströmen bei Kryptowährungen. Auch die dafür benötigten Fachkräfte können wir gewinnen, weil es die Sache offenbar wert ist.

Die Dunkelziffer von Cybercrime-Opfern ist groß, die Zahl der Anzeigen eher gering. Warum ist das so?

Gerade bei Cybercrime ist das Dunkelfeld überdurchschnittlich stark ausgeprägt. Eine aktuelle Umfrage des Digitalverbands Bitkom zeigt, dass nur 18 Prozent der durch Cybercrime betroffenen Privatpersonen in Deutschland Anzeige erstattet haben.

Bei Firmen als Opfer von Cyber-Kriminellen wird das Anzeigeverhalten gegebenenfalls auch durch falsche Vorstellungen zur Kooperation mit der Polizei beeinträchtigt. Viele sorgen sich um ihre Firmendaten und haben Angst, dass ihr Fall medial publik wird. Ich bemühe mich mit diesen Mythen aufzuräumen. Wir fahren weder mit Blaulicht in die Firmenzentrale noch nehmen wir alle Datenträger mit. Wir schauen bei Cybercrime-Ermittlungen auch nicht auf die Buchhaltung des Unternehmens. Wir werten das Datenmaterial ausschließlich auf Cybercrime-Spuren aus.

Welche Rolle spielt bzw. wird künstliche Intelligenz (KI) künftig bei Cybercrime spielen?

KI erlebt gerade einen Riesenhype und birgt wie alle technische Neuerungen Chancen und Risiken. Täter nutzen KI derzeit vor allem für Phishing-Mails und zum Programmieren von Schadcode-Software. Wir als Behörde setzen KI sehr vorsichtig ein. Derzeit nutzen wir sie vor allem in der Bilderkennung.

Wie kann man sich als Privatperson vor Cyber-Kriminellen schützen?

Privatpersonen empfehle ich sichere und gute Passwörter. Man sollte kein Passwort zweimal vergeben und stets alle Updates und Patches einspielen, um mögliche Sicherheitslücken im Betriebssystem zu schließen. Und am wichtigsten: Der sensible Umgang mit persönlichen Daten. Sollten Sie dennoch Betrugsopfer werden, wenden Sie sich an die Polizei und erstatten Sie eine Anzeige.

Interview: Jürgen Belko