Cyberversicherungen >
< Streamingdienste mit Kindern sicher nutzen

Die neue Abteilung Cybercrime im BKA

Im Team gegen Internetkriminelle

Unternehmen und Behörden werden mit Ransomware oder DDoS-Attacken erpresst

Seit April gibt es im Bundeskriminalamt (BKA) die neue Abteilung „CC“ – Cybercrime. In der Abteilung werden verschiedene Kompetenzen gebündelt, um möglichst effektiv und schlagkräftig gegen Internetkriminelle vorzugehen. Kriminalbeamte, Analysten und IT-Experten mit den unterschiedlichsten Spezialisierungen arbeiten hier Hand in Hand. Carsten Meywirth ist der Leiter der Abteilung Cybercrime. Er erklärt, was die Hauptaufgaben des neuen Bereichs sind.

Ein wichtiger Aufgabenbereich ist vor allem, neue Phänomene und digitale Angriffsmuster im Bereich Cybercrime zu analysieren. Aber auch Ermittlungen gegen kriminelle Akteure, Netzwerke und Strukturen, etwa im Darknet, werden maßgeblich von der neuen Abteilung geführt. „Wir sind dabei für die Bereiche im Rahmen der so genannten „Cybercrime im engeren Sinne“ verantwortlich. Damit sind Straftaten gemeint, die sich gegen IT-Infrastrukturen wie Netze oder Server richten, zum Beispiel durch sogenannte DDoS-Attacken oder die Verbreitung von Ransomware“, erklärt Carsten Meywirth. Mit Straftaten der „Cybercrime im weiteren Sinne“ beschäftigen sich andere Abteilungen des Bundeskriminalamts. Dazu gehören etwa Straftaten, bei denen das Internet quasi als Hilfsmittel genutzt wird, beispielsweise für Drogenhandel oder die Verbreitung von Kinderpornografie. „Die Ermittlungen bei Cybercrime im engeren Sinne finden vor allem digital statt, da sich auch die Kriminellen bei ihren Taten in erster Linie in der digitalen Welt bewegen“, so der BKA-Experte. Zuständig ist die neue Abteilung Cybercrime außerdem, wenn Behörden des Bundes sowie Bereiche, die zu den Kritischen Infrastrukturen zählen wie zum Beispiel

Banken, Krankenhäuser, Flughäfen oder Versorgungswerke angegriffen werden.

Arbeit im „Tandem“

Carsten Meywirth, Leiter der Abteilung Cybercrime im BKA

Um möglichst effektiv gegen Cyberkriminelle vorgehen zu können, arbeiten in der Abteilung verschiedene Spezialisten. Rund 70 Prozent der Abteilung sind Polizeibeamtinnen und -beamte, die restlichen 30 Prozent der Mitarbeiterinnen und Mitarbeiter sind vor allem Cyber-Analysten, die ein IT-Studium absolviert haben, sowie andere IT-Experten wie Big-Data-Experten oder Administratoren, die sich um die IT-Infrastruktur kümmern. „Wir fahren hier in der Abteilung eine Art Tandem-Modell. Das heißt, wir haben auf der einen Seite ausgebildete Polizeivollzugsbeamte, deren klassische Kenntnisse zur Strafverfolgung bei uns in der täglichen Arbeit um spezielle Cyber-Kompetenzen ergänzt werden. In den Ermittlungs- und Auswerteverfahren gegen Cyberkriminelle arbeiten die Polizeibeamtinnen und -beamten im Tandem mit einem unserer Cyber-Analysten, die wir als IT-Fachkraft extern gewonnen haben und denen wir wiederum das kriminalistische Handwerkszeug näherbringen“, erklärt Carsten Meywirth. Dieses Vorgehen hat sich bewährt. „Die Teammitglieder ergänzen sich perfekt in ihren Kenntnissen und Kompetenzen. Man kommt nur gemeinsam weiter. Das sorgt unter anderem dafür, dass die Motivation bei der Arbeit enorm hoch ist“, betont Meywirth. Ein weiteres besonderes Merkmal ist die enge Zusammenarbeit mit Behörden aus dem Ausland. „Cybercrime ist internationale Kriminalität. Daher sind auch wir international sehr gut vernetzt. Dabei pflegen wir insbesondere Kontakte innerhalb Europas, aber auch mit den Vereinigten Staaten von Amerika oder Australien. Kontakte gibt es aber auch in den asiatischen Raum.“

Erpressung und „Cybercrime as a service“

Ein Bereich, der die Expertinnen und Experten häufig beschäftigt, sind moderne Formen von Erpressung, zum Beispiel mithilfe von DDoS-Attacken. Dabei wird etwa die Online-Präsenz einer Bank von Cyberkriminellen so lange mit Anfragen bombardiert, bis der Server herunterfährt und dann zum Beispiel das Online-Banking für Kunden nicht mehr zur Verfügung steht. „Die Täter fordern dann von dem Bankunternehmen ein Lösegeld, um diese Attacken zu stoppen und die Online-Präsenz wieder verfügbar zu machen“, erklärt Meywirth. Auch Ransomware wird von Cyberkriminellen häufig eingesetzt, um Unternehmen zu erpressen. Dabei wird Schadsoftware eingespielt, die bestimmte Daten verschlüsselt, sodass das Unternehmen keinen Zugang mehr dazu hat. Zudem drohen die Täter zunehmend damit, die Daten weiterzuverkaufen. Solche Erpressungs-Software wird von Kriminellen auch im Darknet zum Kauf angeboten, das heißt, Täter müssen sie nicht selbst programmieren, sondern können sie einsatzbereit einkaufen. „Diesen Bereich nennen wir „Cybercrime as a service“. Auch hier ist meine Abteilung verstärkt tätig“, betont Meywirth.

Weitere Spezialisierung und Expertise

Das BKA blickt bei der Bekämpfung von Cybercrime bereits auf langjährige Erfahrung zurück. Schließlich startete man schon Mitte der 1990er Jahre in einem kleinen Arbeitsbereich der Abteilung „Organisierte und Allgemeine Kriminalität“ unter der Bezeichnung „Informations- und Kommunikationskriminalität“. Im Jahr 2013 entstand dann die Gruppe „Cybercrime“ mit über 100 Mitarbeiterinnen und Mitarbeitern. Diese Gruppe bildet nun den fachlichen Grundstein der neuen Abteilung, die bis zum Jahr 2022 auf rund 280 Beschäftigte anwachsen soll. „Wir setzen dabei auch in Zukunft neben den eigenen Kompetenzen auf die Expertise von externem IT-Fachpersonal. Ich denke, dass das BKA hier ein spannendes Arbeitsumfeld

bietet, das sich von dem eines Wirtschaftsunternehmens abhebt. Schließlich ist man bei uns an polizeilichen Ermittlungen an vorderster Front beteiligt“, so Carsten Meywirth.
SBa (26.06.2020)

Folgende Artikel könnten Sie auch interessieren:

- Cyber-Betrugsmasche „Jackpotting“
- Bestellt und nichts geliefert
- Sexting - Nacktfotos im Netz

Alle Artikel dieser Kategorie

Weitere Infos zum Thema Internet und Mobil

Experten beraten individuell zur Internetnutzung Jugendlicher

Neues Hilfe-Portal für Eltern und Lehrer

Die Bundeszentrale für gesundheitliche Aufklärung (BZgA) bietet...[mehr erfahren]

Internetkriminelle wollen an ihre Zugangsdaten für Online-Geschäfte gelangen

Phishing – so können Sie sich schützen

„Phishing“ ist ein Kunstwort, das sich aus den englischen Begriffen...[mehr erfahren]

Berliner Pilotprojekt zur Gesichtserkennung erfolgreich

Wie Computer lernen, Menschen zu erkennen

Biometrische Systeme wie Fingerabdruck- oder Gesichtsscanner werden...[mehr erfahren]

Shoppen und Banken von Zuhause - aber sicher!

Bankgeschäfte und Einkaufen im Netz

Keine Parkplatzprobleme, eine freie Zeiteinteilung, keine...[mehr erfahren]

Regeln zu Bild- und Videorechten

Die Polizei und das Recht am eigenen Bild

Immer öfter werden Polizisten bei der Ausübung ihres Berufes gefilmt...[mehr erfahren]