Cybercrime: Angriffe aus dem Netz

Waffenhandel, Kinderpornografie, Daten-Phishing, Verbreitung von Schadsoftware, Betrug-E-Mails: alles illegale Aktivitäten, die sich in der digitalen Welt immer weiter ausbreiten. Zusammen-gefasst werden sie unter dem englischen Begriff Cybercrime.

Eine allgemein gültige Definition für Cybercrime gibt es nicht. Die Polizei beschreibt diese Form der Kriminalität als »Straftaten, die sich gegen das Internet, Datennetze, informationstechnische Systeme oder deren Daten richten (Cybercrime im engeren Sinne) oder die mittels dieser Informationstechnik begangen werden.« Täglich entwickeln sich digitale Angriffsmethoden, technische Arbeitsmittel und deren Nutzung weiter, die innerhalb kürzester Zeit von weltweit agierenden Tätern aufgegriffen werden. Der ökonomische Schaden, den Cyberkriminelle durch ihre Angriffe auf Computer und mobile Endgeräte von Privatpersonen, Unternehmen und Institutionen anrichten, beträgt mehrere Milliarden Euro. Im Cybercrime sei »wie in kaum einem anderen Deliktsbereich eine kontinuierlich steigende Kriminalitätsentwicklung zu verzeichnen«, so der Hinweis des

Bundeskriminalamtes (BKA) auf seiner Website.

Zentrale Ansprechstelle im Dezernat 47

Im reinland-pfälzischen Landeskriminalamt (LKA) wurde 2012 in Mainz das Dezernat 47 zur Bekämpfung von Cybercrime eingerichtet. Zu seinen Aufgaben gehören, neben seiner Zentralstellenfunktion, die Bearbeitung von besonderen Ermittlungsverfahren von Cybercrime und die anlassunabhängige Recherche in Datennetzen. Dem Dezernat angegliedert ist die Zentrale Ansprechstelle Cybercrime (ZAC), an die sich öffentliche wie nicht-öffentliche Einrichtungen und Wirtschaftsunternehmen in Rheinland-Pfalz bei Cyberangriffen wenden können. Die ZAC-Hotline nimmt jede Anzeige auf, prüft sie und leitet den Fall an die zuständige Stelle im Dezernat weiter.

Schwierige Strafverfolgung

Unabhängig von der Größe der Firma oder Institution spiele sich dieser Vorgang ab, sagt Sabina Jülich, ZAC-Koordinatorin und Ansprechpartnerin im Bereich Grundsatz/Strategie im Dezernat 47. »Wir differenzieren hier nicht.« Liegt eine Straftat vor, werden der Firmeninhaber oder Einrichtungsleiter und der IT-Bereich kontaktiert. »Dann versuchen unsere Ermittler und die IT-Spezialisten die Ermittlungen so durchzuführen, dass das Unternehmen möglichst wenig in seinen Abläufen gestört wird.«

Im besten Fall läuft es bei der Strafverfolgung auf die Ergreifung des Täters hinaus. Aber noch, so Jülich, sei die Aufklärungsquote gering. Dies läge zum einen an der rasanten Evolution der Technologien, die Cyberkriminelle nutzten, und zum anderen an der zunehmenden Professionalisierung und Internationalisierung der Delikte. Um ihre Standards und Ressourcen für die Strafverfolgung zu verbessern, setzt die ZAC auf Cybercrime-Kooperationen mit anderen Sicherheitsbehörden sowie externen Partnern aus Wirtschaft und Wissenschaft. Zudem informiert Jülich in ihren Vorträgen bei Firmenverbänden über Präventionsmaßnahmen gegen Cybercrime und gibt Handlungsanleitungen, wie sich Unternehmen zum Beispiel bei Erpressungen durch Schadsoftware verhalten sollten. »Wir möchten außerdem vermitteln, dass es sich bei der ZAC um eine vertrauensvolle Stelle handelt«, ergänzt Jülich. Denn nicht selten hätten Firmen nach einem Cyberangriff Angst vor einem Imageschaden.

| KH

ZAC-Hotline: 06131 65 2565 (nur für Wirtschaftsunternehmen, Behörden und Einrichtungen),
www.polizei.rlp.de/de/aufgaben/kriminalitaet/kriminalitaetsbekaempfung/cybercrime