Zentrale Ansprechstelle Cybercrime (ZAC)

Merkblatt
zum Vorgehen in Fällen von Cybercrime

IHK Landesarbeitsgemeinschaft der Industrie- und Handelskammern des Landes Brandenburg

Stand: 14.12.2016

Straftaten im und durch das Internet kennen keine Grenzen und finden sowohl länder-, als auch branchenübergreifend statt. Um dem Phänomen „Cybercrime“ erfolgreich begegnen zu können, ist nicht nur eine intensive innerpolizeiliche Zusammenarbeit notwendig. **Auch die vertrauensvolle Zusammenarbeit mit der Wirtschaft muss weiter ausgebaut werden, um der schnellen Entwicklung in diesem Kriminalitätsbereich Rechnung zu tragen.**

Cybercrime umfasst die Straftaten, die sich gegen das Internet, Datennetze bzw. deren Daten richten oder die mittels dieser Informationstechnik begangen werden. Das umfasst u. a. folgende Phänomene:

- Angriffe auf die Verfügbarkeit von Webseiten, Internetdiensten und Netzwerken (DDoS-Angriffe),
- Digitale Erpressung unter Einsatz sogenannter Ransomware,
- Verbreitung von Schadsoftware z. B. per E-Mail oder Drive-by-Downloads,
- Diebstahl und Missbrauch digitaler Identitäten z. B. durch Social Engineering,
- Übernahme von Händler- und Kunden-Accounts bei Online-Verkaufsplattformen, um betrügerische Angebote von Waren,
  Immobilien etc. einzustellen und den Kaufbetrag per Vorkasse (Warenbetrug) zu kassieren,
- Angriffe auf das Onlinebanking, CEO-Fraud (Betrug),
- Massenhafte Fernsteuerung von Computern (Botnetze) und IoT-Geräten (Internet of Things),
- Gefährdung mobiler Endgeräte.

Die Nutzung digitaler Informations- und Kommunikationsmittel ist zu einer unabdingbaren Voraussetzung des modernen gesellschaftlichen und wirtschaftlichen Lebens geworden. Zugleich sind mit der zunehmenden Vernetzung internetfähiger Geräte im privaten wie auch professionellen Bereich die Manipulations- und Angriffsmöglichkeiten für Cyberkriminelle, z. B. durch das gezielte Ausnutzen von Schwachstellen in den IT-Systemen, weiter gestiegen. Zudem stellt die Zunahme diverser Formen des Waren- und Warenkreditbetruges im Internet weiterhin eine ernstzunehmende Bedrohung für die Internetnutzer und Betreiber von eCommerce-Portalen dar.

Was ist zu tun, wenn Sie Anhaltspunkte für das Vorliegen eines Cybercrime-Deliktes feststellen? Verständigen Sie sich mit Ihrem Systemadministrator. Wenden Sie sich vertrauensvoll möglichst innerhalb von 24 Stunden an:

- die jeweils örtlich zuständige Polizeidienststelle
  - bei Fällen der Internetkriminalität (z. B. Waren-/Warenkreditbetrug, Beleidigung)
  - bei Fällen der einfachen Cybercrime (z. B. Ausspähen von Kundendaten und Administrator-Passwörtern)

- an die Zentrale Ansprechstelle Cybercrime (ZAC) - **Telefon: 03334 388-8686**
  - bei herausgehobenen Cybercrime-Delikten (z. B. DDoS-Angriffe, Hackerangriffe auf Firmenserver und Datenbanken, Computersabotage, Sperrung von Webseiten, SQL-Injection)

Welche Informationen sollten Sie bereithalten?
Nach Feststellung eines Cybercrime-Falles benötigt die Polizei für die Erstattung einer Strafanzeige folgende Angaben:

- Name, Anschrift, Erreichbarkeit der geschädigten Firma und Ihres Systemadministrators
- Was ist wann und wo geschehen?
- Gibt es Hinweise/Kontakte zu möglichen Tätern bzw. zum Tatmotiv?
- Welche IT-Systeme/Server bzw. URLs sind betroffen?
- Gibt es digitale Spuren/Beweismittel?
- Wurden bereits Lösegeldzahlungen an Erpresser geleistet?
- Erfolgte eine Kompromittierung ihrer IT-Systeme durch Schadsoftware?
- Wie groß ist der bisher festgestellte Schaden bzw. Umsatzausfall?
- Wurden personenbezogene Daten (z. B. E-Mail-Adressen, IP-Adressen) bekannt?
- Gibt es Hinweise auf andere Geschädigte?

Zentrale Ansprechstelle Cybercrime, 16225 Eberswalde, Tramper Chaussee 1
Telefon: 03334 388-8686, Telefax: 03334 388-8609
ZAC@polizei.brandenburg.de

außerhalb der Bürodienstzeit:
Telefon: 0331 283-3035
Telefax: 0331 283-3059