Polizeipräsidium
Land Brandenburg

Merkblatt
zum Vorgehen in Fällen von Cybercrime

IHK Landesarbeitsgemeinschaft der Industrie- und Handelskammern des Landes Brandenburg

Stand: 04.06.2015

Unter „Cybercrime“ oder „Internet-Kriminalität“ versteht man Straftaten, die unter Ausnutzung moderner Informations- und Kommunikationstechnik oder gegen diese begangen werden. Das sind:

- alle Straftaten, bei denen die EDV zur Planung, Vorbereitung oder Ausführung einer Tat eingesetzt wird oder wurde (Computerkriminalität),
- Straftaten im Zusammenhang mit Datennetzen, wie z. B. dem Internet, und
- Fälle der Bedrohung von Informationstechnik. Dies schließt alle widerrechtlichen Handlungen gegen die Integrität, Verfügbarkeit und Authentizität von elektronisch gespeicherten oder übermittelten Daten ein (z. B. Hacking, Computersabotage, Datenveränderung, Missbrauch von Telekommunikationsmitteln).

Das Gefährdungs- und Schadenspotential des Phänomens „Cybercrime“ ist unverändert hoch. Neben Angriffen auf IT-Systeme und mobile Endgeräte werden zwischenzeitlich auch sämtliche Formen und Arten von digitalen Identitäten ausgespäht und illegal eingesetzt. 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 388-0
  - 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 Eintritt eines Schadensfalles 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?
  - Ein unberechtigter Nutzer hat sich in das System eingeloggt bzw. nutzt das System.
  - Es laufen ungewöhnliche Prozesse auf dem System, die große Mengen an Systemressourcen in Anspruch nehmen.
  - Das System ist von einem Virus, Wurm oder Trojaner befallen (evtl. mit einer Geldforderung verbunden).
  - Ein Nutzer versucht von außerhalb, z. B. durch intensives Portscanning, in das System einzudringen.
  - Der Internetauftritt, der Online-Shop oder das E-Mail-Postfach ist lahmgelegt (DDoS-Attacke). Innerhalb kurzer Zeit erreicht eine große Menge an Datenpaketen das System.
- Welche Systeme/Server bzw. URLs sind betroffen?
- Auf welche Server (-Standorte) wurden Daten übertragen?
- Gibt es Hinweise/Kontakte zu möglichen Tätern?
- Wurden bereits Lösegeldzahlungen an Erpresser geleistet?
- Wie groß ist der bisher festgestellte Schaden bzw. Umsatzausfall?
- Gibt es Hinweise auf andere Geschädigte?

Zentrale Ansprechstelle Cybercrime, 16225 Eberswalde, Tramper Chaussee 1
Telefon: 03334 388-0, Telefax: 03334 388-8609
Cybercrime.FDLKA@polizei.brandenburg.de

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