Checkliste für den Kontakt zur ZAC LKA NRW

Notwendige und wünschenswerte Vorbereitungen vor einer Kontaktaufnahme

Ansprechpartner

In der ersten Phase der Erkenntnisgewinnung ist die Aufstellung aller relevanten Ansprechpartner essenziell. Die Erreichbarkeit sollte sowohl telefonisch (Mobil und Festnetz) als auch per E-Mail gewährleistet sein.

- Technischer Ansprechpartner
  Es wird ein Ansprechpartner benötigt, der einen Überblick über die IT relevanten Prozesse im Unternehmen hat und auch unmittelbaren Zugriff auf die Systeme (z.B. zur Erhebung von Log- und Protokolldateien) gewährleisten kann. Wurde die Administration der IT Technik von einem externen Dienstleister übernommen, so sollte dieser kontaktiert und zur Zusammenarbeit mit den Ermittlungsbeamten aufgefordert werden.

- Vertreter des Unternehmen
  Der Vertreter des Unternehmens soll der Polizei als Ansprechpartner für alle grundsätzlichen Fragen der Ermittlungszusammenarbeit dienen. Er sollte in der Lage sein, Entscheidungen zu treffen, oder diese zeitnah herbeiführen können.

- Justizieller Ansprechpartner
  Grade in der ersten Ermittlungsphase besteht häufig Bedarf, datenschutz- und strafprozessrechtliche Fragen zu klären. Dafür benötigen die eingesetzten Polizeibeamten und die involvierte Staatsanwaltschaft einen entscheidungsberechtigten Ansprechpartner.

- Alle weiteren relevanten Personen
  Personen, die für Ermittlungsmaßnahmen oder dem grundsätzlichen Verständnis vorliegender Besonderheiten relevant sind, sollten benannt werden und ebenfalls erreichbar sein.

Kontakt (24/7):

Landeskriminalamt Nordrhein-Westfalen | Cybercrime Kompetenzzentrum | cybercrime.lka@polizei.nrw.de | 0211 - 939 4040

Sachverhalt

Die Transparenz vorliegender Informationen ist relevant für eine polizeiliche Einschätzung des Sachverhalts. Insbesondere folgende Punkte sollten Beachtung finden:

- Detaillierte Beschreibung des Vorfalls incl. aller getätigten Maßnahmen und einer Zeitleiste. Ist der Vorfall bereits beendet, oder ist weiterer Schaden zu erwarten (z.B. bei andauernden Cyberangriffen)?
- Soweit bereits möglich eine Schadensaufstellung oder eine Abschätzung des erwarteten Schadens / Schadensausmaß.
- Sind Informationen zu Tätern bekannt? Besteht bereits eine Kommunikation mit dem Täter oder hat dieser eine Nachricht hinterlassen?
- Betroffene Systeme, Niederlassungen, Abteilungen

Maßnahmen

Bereits vor dem Kontakt zur Polizei können wichtige Maßnahmen getroffen werden, ohne die eine erfolgreiche Ermittlungsarbeit häufig ausgeschlossen ist.

- Vermeiden des Verlustes von Protokolldateien.
  Häufig speichern IT Systeme Protokolldateien nur innerhalb eines engen Zeitraumes. Sichern sie diese Protokolldateien rechtzeitig oder verlängern Sie den Speicherzeitraum. Ggf. Log-Level erhöhen.
- Wenn möglich legen Sie Snapshots von betroffenen Datenträgern an.
- Ereignisprotokoll
  Bitte führen sie, sobald sie von dem relevanten IT Vorfall erfahren, ein Ereignisprotokoll. Protokollieren sie auch alle Änderungen, die Sie an betroffenen Systemen vorgenommen haben.

Ermittlungen vor Ort

Sollte der Sachverhalt konkrete Ermittlungen vor Ort benötigen, so bitten wir sie, folgende Vorbereitungen zu treffen, die je nach Dauer der Ermittlungen essenziell sind:

- Bereitstellen eines abschließbaren Raums für polizeiliche IT-Forensikmaßnahmen.
- Internetzugang (möglichst Highspeed)
- Parkmöglichkeiten in unmittelbarer Nähe für mehrere Fahrzeuge