Polizeilich festgestellte Cybercrime-Phänomene im Zusammenhang mit COVID-19 (Corona)

Überblick

Vorwort

In diesem Newsletter werden Cybercrime[1]-Phänomene betrachtet, die sich mit der Corona-Pandemie entwickelt bzw. angepasst haben und der Polizei bekannt geworden sind. Aufgrund der andauernden Pandemie wird das Internet deutlich verstärkter genutzt. Neben den eher klassischen Cyberdelikten werden im Bundesgebiet vermehrt Straftaten mit Corona-Bezug festgestellt. Es wird damit gerechnet, dass die Bedrohungslage kurz- bis mittelfristig anhält und die Täter die Situation weiter ausnutzen.

Bislang wurde kein qualitativer Anstieg von kritischen Vorfällen oder schwerwiegende technischen Ausfälle festgestellt.

[1] Straftaten, bei denen Informations- und Kommunikationstechnik zur Planung, Vorbereitung oder Ausführung genutzt wurde.

Phänomene

Phishing

Gegenwärtig werden vermehrt E-Mails im Namen anderer Behörden und Unternehmen versendet, um Daten von den Empfängern abzugreifen. Im Folgenden ein paar Beispiele:

- Geschädigte erhielten E-Mails mit PayPal-Logo. Dem Inhalt nach, sollten aufgrund der Corona-Pandemie „inaktuelle" Konten geschlossen werden. Die Empfänger sollen auf einen Link klicken und ihre Daten überprüfen.

- Es wurden mehrere Sachverhalte angezeigt, in denen E-Mails im Namen der Arbeitsagentur (kurzarbeitergeld@arbeitsagentur.de) gesendet wurden. Das Antworten erfolgt an kurzarbeiter-geld@arbeitsagentur-service.de. Die Täter wollten allem Anschein nach, die Daten der Firmen verwenden, um Kurzarbeitergeld in deren Namen zu beantragen.

- Am 04. Mai 2020 wurden vermehrt E-Mails angezeigt, die im Namen der zuständigen Banken für Soforthilfen versendet wurden. Die Absende-E-Mail-Adressen beginnen mit „corona-zuschuss" und enden auf „.de.com"., wie z. B. **corona-zuschuss**@nbank**.de.com**. Die E-Mails enthalten den Betreff „Corona Zuschuss - Bestätigung und Belehrung" sowie zwei Anhänge mit den Namen „Rechtsbelehrung_Zuschussempfaenger.pdf" und „Bescheinigung_Finanzamt.pdf". Die Täter bauen in dem Schreiben eine Drohkulisse auf und informieren über vorgebliche Straftatbestände bei ungerechtfertigtem Erhalt von Soforthilfen. Sie fordern zu einer elektronischen Kontaktaufnahme im Kontext einer Fördergeld-Rückzahlung auf.

- Darüber hinaus wurden auch E-Mails mit der gleichen Zielstellung im Namen von anderen staatlichen Behörden, wie das Gesundheitsministerium, versendet.

Erpressung

- Bundesweit wurden Droh-E-Mails im Namen „Die Musiker des Staatsstreichorchesters" versendet. Es wird mit dem Angriff auf IT-Infrastrukturen verschiedener Krankenhäuser gedroht.
- Ferner wurden Firmen per E-Mail kontaktiert und mitgeteilt, dass ein Mitarbeiter mit Corona infiziert sei. Es soll ein gewisser Betrag in der virtuellen Währung Bitcoin gezahlt werden, andernfalls werden Behörden darüber informiert.

Versand von Schadsoftware

Per E-Mail wurde Schadsoftware im Namen von Gesundheitsministerien versendet. Die Empfänger werden angehalten ein geändertes Antragsformular in Bezug auf Familien- und Krankenurlaub anzuschauen. Angehangen war der Banking-Trojaner Trickbot, welcher das IT-System nach Informationen durchsucht und diese ausleitet.

Betrug

Im Zusammenhang mit Betrügereien wurden schwerpunktmäßig die nachfolgenden Ausprägungen angezeigt:

- Fake-Shops (Warenbetrug)
  - Es werden online Corona-Impfmittel, Schutzkleidung etc. angeboten, jedoch nicht geliefert.

- Fake-Webseiten
  - Webseiten von Unternehmen (z. B. Pharmazieunternehmen) wurden kopiert und unter einer anderen Domain (z. B. anstelle „.de“ „.com“) veröffentlicht. Anschließend wollten Geschädigte Produkte erwerben, die ebenfalls nicht geliefert wurden.

- Beantragung staatlicher Soforthilfen (Subventionsbetrug)
  - In vielen Bundesländern wurden die offiziellen Webseiten der staatlichen Soforthilfen kopiert und unter anderen Domains veröffentlicht. So beispielsweise bei der sächsischen Aufbaubank (SAB). Die richtige Webseite ist portal.sab.sachsen.de, die von den Tätern registrierte sachsen-sab.de.

  - Das Bundesland NRW setzte Anfang April die Einreichung von Anträgen in Bezug mit den Corona-Soforthilfen aus. Hintergrund waren ebenfalls Nachahmer-Webseiten (z. B. wirtschaft-nrw.info anstelle wirtschaft.info).

Staatliche Soforthilfe in Brandenburg

Die Landesinvestitonsbank in Brandenburg wird ab dem 06.05.2020 ein Antragsportal auf deren Internetseite (https://ilb.de) bereitstellen. Das bisherige Verfahren (Antrag und Anlagen herunterladen, ausfüllen und per E-Mail an soforthilfe-corona@ilb.de. versenden) wird abgelöst. Das vorrangige Ziel ist, den Antragsprozess zu automatisieren, um die Soforthilfen schneller bereitstellen zu können.

Anzeigenerstattung im Land Brandenburg

Wenn Sie von einem der genannten Phänomene oder einer anderen Begehungsweise von Straftaten i. Z. m. COVID-19 (Corona) betroffen sind, wird um Anzeigenerstattung unter www.polizei.brandenburg.de/onlineservice/auswahl_Strafanzeige oder bei der örtlich zuständigen Polizeidienststelle gebeten.

Als Unternehmen oder Behörde steht Ihnen im Zusammenhang mit Straftaten, rund um das Thema Cybercrime und Informationstechnik, auch die Möglichkeit der Anzeigenerstattung über die Zentrale Ansprechstelle Cybercrime (ZAC) zur Verfügung.

Impressum
Polizeipräsidium - Landeskriminalamt
Cyber-Competence-Center – Zentrale Ansprechstelle Cybercrime (ZAC)
16225 Eberswalde, Tramper Chaussee 1
ZAC -Telefon: 03334 388 8686 (Mo-Do 09:00 bis 16:00 Uhr und Fr 09:00 bis 14:00 Uhr)
zac@polizei.brandenburg.de