Bundeskriminalamt

# PRESSEMITTEILUNG
des Bundeskriminalamtes

Thaerstraße 11
65193 Wiesbaden

Tel. +49 611 55-13083
pressestelle@bka.bund.de
www.bka.de

30.09.2020

## Cybercrime in Deutschland nimmt weiter zu

**Bundeskriminalamt stellt Bundeslagebild 2019 sowie Sonderauswertung zu Cybercrime in der Corona-Krise 2020 vor**

100.514 Fälle von Cybercrime im engeren Sinne registrierte die deutsche Polizei in 2019, was einem Anstieg von über 15 Prozent gegenüber der Vorjahreszahl entspricht (2018: 87.106 Fälle). Wie aus dem heute vom Bundeskriminalamt (BKA) veröffentlichten „Bundeslagebild Cybercrime 2019“ hervorgeht, erreicht die Anzahl der polizeilich bekannten Taten damit einen neuen Höchststand.

Die Schäden, die durch entsprechende Taten entstehen, sind hoch. So schätzt der Branchenverband BITKOM, dass der Wirtschaft 2019 ein Schaden von über 100 Milliarden Euro durch Cyberangriffe entstanden ist. Neben Wirtschaftsunternehmen sind öffentliche Einrichtungen bevorzugte Ziele der Täter, die sich hier hohe kriminelle Gewinne erwarten.

Die größte Gefahr geht weiterhin von Angriffen mittels sogenannter Ransomware aus. Diese Software verschlüsselt die Daten auf dem angegriffenen Rechner. Für deren Entschlüsselung fordern die Täter meist einen Geldbetrag, der in der Regel in Form von Bitcoins zu entrichten ist. Seit dem vergangenen Jahr beobachtet das BKA mit der sogenannte „Double Extortion“ einen neuen Modus Operandi, bei dem die Täter die IT-Systeme ihrer Opfer nicht nur mittels Ransomware verschlüsseln, sondern im Zuge der Attacken auch sensible Daten erbeuten und damit drohen, diese zu veröffentlichen.

Die Polizei stellte 2019 insgesamt 22.574 Tatverdächtige fest – über 2 Prozent mehr als noch in 2018 (22.051 Tatverdächtige). Cyberkriminelle sind in der Regel international vernetzt und agieren arbeitsteilig. Hinzu kommt, dass sie sich neuen Situationen flexibel anpassen.

Diese Flexibilität ließen die Täter auch im Zusammenhang mit der COVID-19-Pandemie erkennen, wie aus der Sonderauswertung „Cybercrime in Zeiten der COVID-19-Pandemie“ hervorgeht. In der heute ebenfalls veröffentlichten Analyse des Zeitraums März bis August 2020 wird beispielsweise auf unmittelbar nach Beginn der Pandemie erstellte Webseiten eingegangen, die in Anlehnung an die Internetpräsenzen staatlicher Stellen etwa mit Informationen und Beratungsgesprächen zur

Corona-Soforthilfe warben. Durch Betätigung von Schaltflächen auf den betreffenden Webseiten wurden die Computer der Besucher mit Malware infiziert. Ähnlich erging es Empfängern von E-Mails, die scheinbar von staatlichen Stellen oder Banken stammten und Informationen zum Thema „Corona“ enthielten. Beim Öffnen eines Anhangs wurde der Computer der Betroffenen mit Schadsoftware infiziert.

Die hohe Zahl der Straftaten und die vielfältigen Modi Operandi im Zuge der COVID-19-Pandemie zeigen, dass es sowohl für Mitarbeiterinnen und Mitarbeiter von Unternehmen als auch Privatpersonen wichtig ist, ihre Daten vor dem Zugriff von Cyberkriminellen zu schützen. Dazu gehört ein aktueller Virenschutz genauso wie sichere Passwörter und regelmäßige Backups.
Wichtig ist aber auch, bei E-Mails von unbekannten Absendern skeptisch zu bleiben, auch wenn diese den Eindruck erwecken, von einer Behörde, Bank oder Bekannten versandt worden zu sein. Aufforderungen zu Geldzahlungen sollte niemals nachgekommen werden. Betroffene von Cybercrime sollten vielmehr möglichst zeitnah die Polizei informieren. Denn nur wenn die Polizei von Cyberstraftaten erfährt, kann sie die Täter ermitteln und die Begehung weiterer Straftaten verhindern.

Martina Link, Vize-Präsidentin beim Bundeskriminalamt:

*„Mit der Einrichtung der Abteilung Cybercrime hat das Bundeskriminalamt die Bekämpfung der Kriminalität im Netz weiter gestärkt. Ein wichtiger Aspekt unserer Arbeit ist dabei die Analyse. Denn nur wenn wir wissen, wie die Cyberkriminellen vorgehen, können wir darauf zielgerichtet reagieren. Die heute veröffentlichte Sonderauswertung zu Cybercrime in Zeiten der COVID-19-Pandemie ist ein gutes Beispiel dafür. Unsere gewonnenen Erkenntnisse setzen wir auch bei Ermittlungen ein. Die Ziele sind klar: Kriminelle Netzwerke aufdecken, Strukturen zerschlagen und Tatverdächtige überführen. Unser Anspruch ist es, den Täterinnen und Tätern stets einen Schritt voraus zu sein. Daher werden wir unsere Kapazitäten im Bereich Cybercrimebekämpfung weiter ausbauen.“*