Bayerisches Staatsministerium des
Innern, für Sport und Integration

Rede des Bayerischen Staatsministers des
Innern, für Sport und Integration, Joachim Herrmann,

anlässlich der Pressekonferenz Cybersicherheit / Cybercrime
in Bayern 2019

am 13. Juli 2020 in München

Es gilt das gesprochene Wort!

Einleitende Worte

Die Themen Cybercrime und Cybersicherheit betreffen viele Ressorts. Ich danke daher meinen Kollegen, – Dir liebe Judith, lieber Albert und lieber Georg – und Ihnen, lieber Herr Dr. Körner, dass Sie meine Initiative zu dieser gemeinsamen Pressekonferenz sofort unterstützt haben.

Seit Beginn der Corona-Pandemie werden nicht nur die Belastungsgrenzen von Krankenhäusern, Polizei und Rettungsdiensten ausgereizt. Auch die Strukturen und Angebote der bayerischen Behörden und Einrichtungen mit Cybersicherheitsaufgaben werden einer besonderen Bewährungsprobe unterzogen.

Denn den rapiden Anstieg der Internetnutzung in den letzten Wochen und Monaten *(Rekorddatenvolumen lt. DE-CIX im März 2020: 9,1 Tbit/s; Dezember 2019: 8,1 Tbit/s)* machen sich Cyberakteure jedweder Art zunutze. Dadurch ergibt sich zugleich eine erhöhte Gefährdung durch Cyberangriffe.

Entwicklung Tatmittel Internet

Die aktuellen Zahlen der Polizeilichen Kriminalstatistik 2019 belegen eine deutliche Zunahme der Straftaten im Deliktsbereich „Cybercrime“. Die mit dem Tatmittel Internet begangenen Straftaten wie Betrugsdelikte oder Beleidigungen und Bedrohungen mittels E-Mail, aber auch die Verbreitung und Besitzverschaffung kinderpornografischer Inhalte stiegen im letzten Jahr um 3.280 Fälle beziehungsweise um 12,4 % auf 29.717 Delikte. Bereits 2018 war ein Anstieg der Fallzahlen um 605 *(+ 2,3%)* auf 26.437 Fälle zu verzeichnen. Dabei gehen wir weiterhin von einem hohen Dunkelfeld aus.

Der Schwerpunkt im Deliktsbereich „Cybercrime“ lag 2019 mit 19.995 Fällen und einem Anstieg von + 10,3 % *(2018: 18.125 Fälle)* eindeutig in der Deliktsgruppe des Betruges. Konkret beim Waren- und Warenkreditbetrug gab es eine Steigerung von + 13,8 % *(2018: 11.223 Fälle; 2019: 12.776 Fälle)* – eine Entwicklung, die sich in der Corona-Zeit noch verstärkt hat!

Ebenso ist beim Identitätsdiebstahl ein starker Anstieg *(Ausspähen von Daten + 8,5 %; Urkundenfälschung + 11,0 %; jeweils mit Tatmittel Internet)* festzustellen. Hierbei werden bestehende Accounts „gehackt“ oder neue Accounts mit unrechtmäßig erlangten „echten“ personenbezogenen Daten eröffnet. Anschließend werden über diese Accounts missbräuchlich Transaktionen im Online-Handel getätigt.

Cybercrime im engeren Sinne

Auch im Deliktsbereich „Cybercrime im engeren Sinne“ wie

- dem Ausspähen von Daten *(§ 202a StGB)*,
- der Datenhehlerei *(§ 202d StGB)* oder
- der Datenveränderung und Computersabotage *(§§ 303a und b StGB),*

ist im Jahr 2019 ein Anstieg von 13.660 *(2018)* auf 14.420 angezeigte Fälle *(2018: 13.660 Fälle)* zu verzeichnen.

Der Gesamtschaden lag im letzten Jahr bei 11,7 Millionen Euro und damit leicht unter dem Schaden des Vorjahres *(2018: 11,9 Millionen Euro).*

Eine detaillierte Aufschlüsselung zur Entwicklung der Cyberkriminalität in Bayern finden Sie auch im aktuellen „Cybercrime – Landeslagebild Bayern 2019“.

Vorkommnisse während Corona-Pandemie

Meine Damen und Herren, ich komme nun zu den besonderen Vorkommnissen im Zusammhang mit der COVID-19-Pandemie:

In den ersten fünf Monaten dieses Jahres weist die PKS für den Phänomenbereich „Tatmittel Internet“ 13.874 Fälle auf. Hier ist im Vergleich zum Vorjahreszeitraum eine Steigerung um rund 14 % *(1.716 Fälle) (2018: 12.158 Fälle)* gegeben. Insbesondere der „Waren- und Warenkreditbetrug“ macht den Großteil der Taten aus und verzeichnet eine Steigerung von 1.195 Fällen *(+ 23,4 %) (2018: 5.113 Fälle; 2019: 6.308 Fälle)*.

Zurückzuführen ist dies auf einen regelrechten „Hype“ des Online-Shoppings in Zeiten des Lockdowns. Im Mai 2020 verzeichnete der Versand- und Internet-Einzelhan-

del in Deutschland im Vergleich zum Vorjahresmonat um 28,7 % höhere Umsätze *(https://de.statista.com/statistik/daten/studie/579708/umfrage/monatliche-umsatzentwicklung-im-versand-und-internet-einzelhandel/)*.

Bei den meisten anderen Straftaten im Bereich Cybercrime sind die Entwicklungen in Anbetracht der COVID-19-Pandemie noch nicht eindeutig absehbar und bedürfen einer Betrachtung über einen längeren Zeitraum.

Aktivitäten der Cyberabwehr

Neben Cyberkriminellen nutzen auch ausländische Nachrichtendienste die Pandemie für ihre Zwecke. Hierbei stehen insbesondere Kritische Infrastrukturen im Fokus. Auch eine Einflussnahme durch großangelegte Desinformationskampagnen zählt zu den Angriffszenarien.

Die auf meine Initiative zu Beginn dieses Jahres neu eingerichtete „Cyberabwehr Bayern“ *(CAZ, ZAC, ZCB, LSI, LDA und LfD)* und das neu beim Bayerischen Landesamt für

Verfassungsschutz angesiedelte Cyber-Lagezentrum hatten hier nun alle Hände voll zu tun. Sie haben ihre erste „Feuerprobe“ erfolgreich bestanden.

Bei der Cyberabwehr Bayern *(CAB)* handelt es sich um eine behördeninterne Informations- und Kooperationsplattform. Der Dienstbetrieb der Cyberabwehr wird durch das Lagezentrum beim Landesamt für Verfassungsschutz sichergestellt.

Seit Jahresbeginn haben sich die Teilnehmer der Cyberabwehr und das Cyber-Lagezentrum in rund 30 Lagebesprechungen und fünf Sonder-Besprechungen zu insgesamt 75 cyberrelevanten Sachverhalten ausgetauscht. Hierbei haben sie zahlreiche weitere Schutzmaßnahmen zur Verbesserung der Cybersicherheit in Bayern angestoßen und dadurch das Informationsniveau zur Cyber-Sicherheitslage Bayern wesentlich gestärkt.

Schadsoftware in elektronischen Patientenakten

So wurde bei einem Angriff auf eine Klinik im europäischen Ausland ein neuartiger Modus Operandi verwendet, bei dem die Schadsoftware in elektronischen Patientenakten versteckt war.

Als schnelle Reaktion hierauf stimmten sich die Teilnehmer der Cyberabwehr untereinander ab und starteten eine großflächige Sensibilisierungsmaßnahme für bayerische Kliniken und Krankenhäuser zu dieser neu im Umlauf befindlichen Schadsoftware.

Zusammenfassend ist festzustellen, dass auch aufgrund der schnellen Abstimmungsprozesse innerhalb der CAB und der daraus resultierenden behördlichen Warnhinweise bislang kein erfolgreicher Ransomware-Angriff auf Kliniken in Bayern bekannt wurde.

Warnung vor Fake-Webseiten bei Corona-Sofortgeldern

Für Antragsteller von Corona-Soforthilfegeldern gab es Warnmeldungen zu Fake-Webseiten. Diese zeigen, dass wir die staatliche Handlungsfähigkeit in diesem

Bereich wirkungsvoll verstärkt haben. Bei dieser Unterstützungsaktion hat die CAB in Zusammenarbeit mit dem Landeskriminalamt bayerische Unternehmen, Kammern sowie Branchenverbände gezielt angesprochen und die Prüf- und Auszahlungsprozesse für Corona-Soforthilfen einer Schwachstellenanalyse unterzogen.

Bayern ist wohl auch deshalb nicht so stark wie andere Bundesländer von dieser Betrugsmasche betroffen.

Hinweis auf Flyer

In dem Flyer „Cybersicherheit für bayerische Behörden und Unternehmen – An wen wende ich mich?“ finden Sie weitere Informationen zur Cyberabwehr Bayern.

Speicherung von IP-Adressen

Meine Damen und Herren, die Aufklärung von Straftaten im Internet und insbesondere bei Kinderpornographie ist nur möglich, wenn man die Strafverfolgungsbehörden mit den richtigen Ermittlungsinstrumenten ausstattet. Aus diesem Grunde

setze ich mich mit Nachdruck für die Speicherung von IP-Adressen ein und halte sie unter Datenschutzgesichtspunkten auch für akzeptabel. Ich übergebe nun das Wort an meinen Kollegen Georg Eisenreich.