Gastbeitrag von Dirk Hintermeier

Cyberkriminalität – eine zweite Pandemie?

Eine Arztpraxis ohne Computer ist kaum vorstellbar. Ob Administration, medizinische Geräte, Materialwirtschaft oder Vernetzung und mobile Kommunikation, die vielen Anwendungsmöglichkeiten bergen Gefahren und können zum Einfallstor für Cyberkriminelle werden. Lesen Sie den Fachbeitrag eines Experten vom Hessischen Landeskriminalamt.

HOHES DUNKELFELD IM BEREICH DER INTERNETKRIMINALITÄT

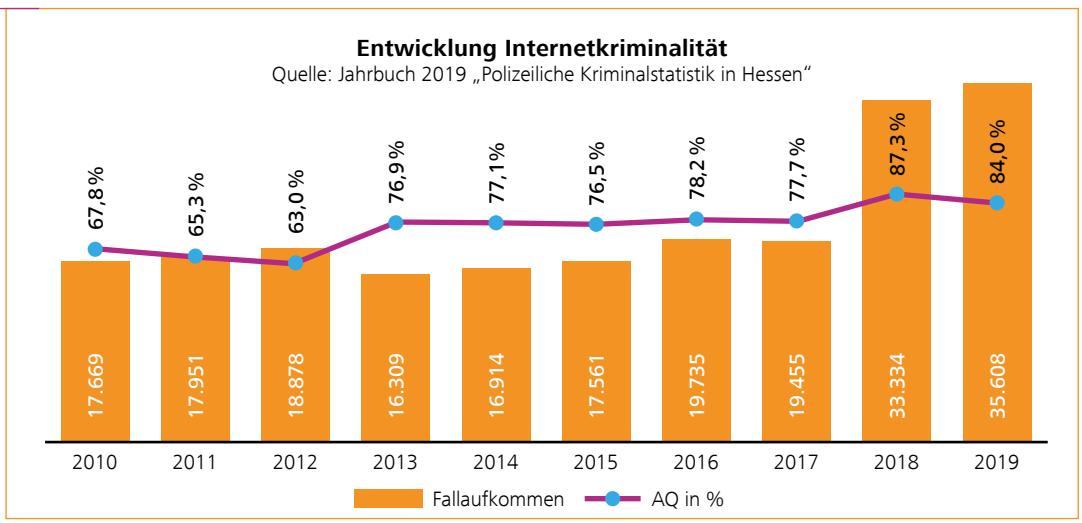
Die aktuellen Fallzahlen der Hessischen Kriminalstatistik zeigen seit 2018 einen sprunghaften Anstieg der Internetkriminalität im Vergleich zu den Vorjahren. Im Jahr 2019 wurden in Hessen insgesamt 35.608 Fälle von Internetkriminalität erfasst. Die Aufklärungsquote (AQ) lag bei 84,0 Prozent (siehe Grafik).

Die tatsächliche Zahl der Straftaten dürfte weit höher sein, da viele Taten nicht zur Anzeige kommen. Außerdem ist mit einem hohen Dunkelfeld zu rechnen. Die Kriminalstatistik erfasst zudem nur Fälle, in denen eine Täterin bzw. ein Täter von einem Ort in Hessen agiert und nicht etwa, ob das Opfer aus Hessen stammt. Nicht berücksichtigt werden zudem aus dem Ausland handelnde Täter.

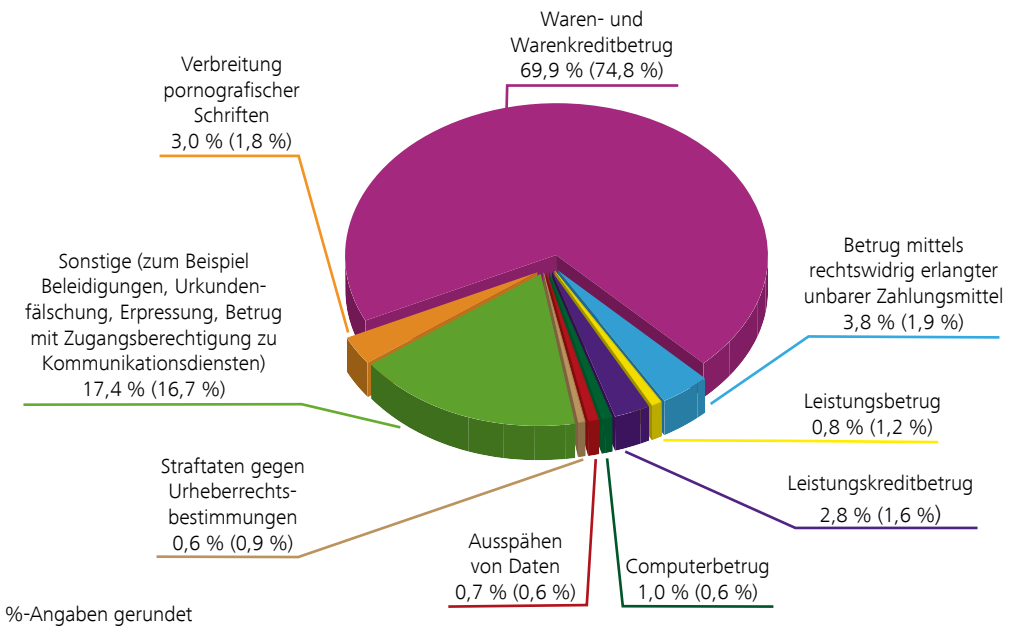
STATISTISCH ERFASST SIND EINBRUCH, BETRUG UND BELEIDIGUNG

Betrachtet man die Struktur der Internetkriminalität im vergangenen Jahr, handelt es sich in fast 70 Pro-

Übersicht zur Entwicklung der Internetkriminalität, zu Fallzahlen und Aufklärungsquoten.



Struktur der Internetkriminalität 2019
Quelle: Jahrbuch 2019 „Polizeiliche Kriminalstatistik in Hessen“



%-Angaben gerundet

Hier eine Übersicht zur Struktur der Internetkriminalität 2019. Die Zahlen aus 2018 finden sich in den Klammern.

zent der Fälle um Waren- und Warenkreditbetrügereien. Also die Fälle, bei der Ware bezahlt, dann jedoch nicht geliefert wird und es auch nicht zu einer Rückzahlung des Geldes kommt.

Arztpraxen waren in den Jahren 2018 und 2019 mit jeweils rund 800 Fällen in der hessischen Kriminalstatistik als Tatörtlichkeit benannt. Die Delikte Einbruch, Betrug und Beleidigung waren am häufigsten. Im Bereich Cybercrime und Praxis ist die Kriminalstatistik leider wenig aussagekräftig. Ein Grund: Strafanzeigen werden meist auf den Namen der praktizierenden Ärztin oder des Arztes als geschädigte Person geführt.

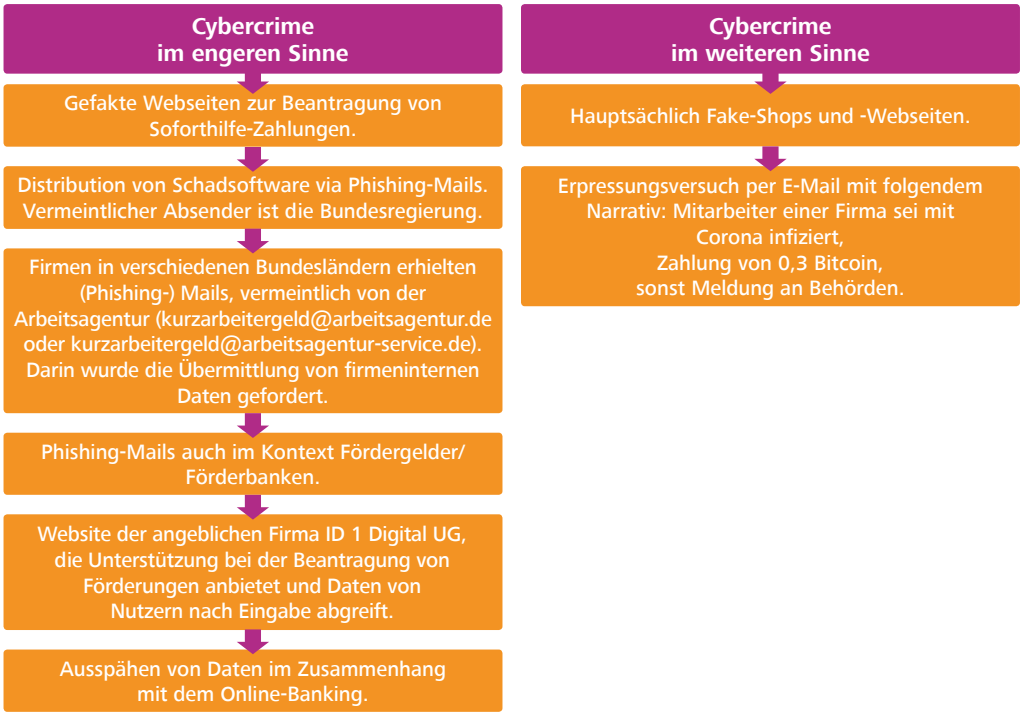
SONDERAUSWERTUNG CYBERCRIME IN ZEITEN DER CORONA-PANDEMIE[1]

In den vergangenen Monaten neu hinzugekommen ist, quasi als logische Konsequenz der Corona-bedingten Einschränkungen, ein Ausweichen in die digitale Welt. Cyberkriminelle sind auf den Zug aufgesprungen und nutzen das Narrativ für ihre typischen Aktivitäten. So hat das Landeskriminalamt Hessen bis Ende Juli 2020 im Corona-Kontext drei Fälle von Cybercrime im engeren Sinne, wie das Ausspähen von Daten, Datenveränderung und -sabotage gemeldet und weitere drei Fallkonstellationen im weiteren Sinne, bei denen IT-Systeme zur Planung, Vorbereitung und Ausführung von Straftaten zum Einsatz kamen. Ein Fall davon sind über 50 Ermittlungsverfahren wegen des Verdachts auf Straftaten im Zusammenhang mit Corona-Soforthilfezahlungen, sprich Subventionsbetrug.

Für die zweite Coronawelle dürften insbesondere das Risiko durch maliziöse bzw. riskante Domains und Dokumente sowie betrügerische Fake-Shops relevant sein. Bekannt geworden sind unter anderem Spam- und Phishing-Kampagnen mit internationalem Charakter. Vermeintliche Absender sind Behörden (zum Beispiel WHO oder Ministerien), Dienstleister (Paket- und Lieferdienste) oder vertrauenswürdige Institutionen und Berufsgruppen, wie beispielsweise die aus dem Gesundheitswesen. Betroffen sind Einkäufe von Schutzausrüstung, Desinfektionsmitteln, Testmaterial, aber auch typischerweise seriöse Informations-Domains und Dashboards, die von Cyberkriminellen gekapert und für Tatzwecke dupliziert werden. Ziel der Cyberkriminellen sind monetäre Mittel und digitale Identitäten.

[1] Bundeskriminalamt: Cybercrime | Sonderauswertung Cybercrime in Zeiten der Corona-Pandemie, September 2020

Fallbeispiele aus der BKA-Sonderauswertung.



Deutlich gestiegen ist die Intensität von DDoS-Angriffen[2], also gezielten Angriffen anderer Computersysteme auf ein Rechnersystem oder eine Homepage. Sie legen die Infrastruktur lahm und können auch ablenken von einem parallel ausgeführten anderen Angriff, zum Beispiel zum Aufspielen von Ransomware.

Beeindruckend sind die Zahlen der IT-Sicherheitsforscher. McAfee beispielsweise hat seit Januar 2020 weltweit über 4,4 Mio. Angriffe mit Covid-19-Bezug festgestellt, davon 200 Tsd. in Deutschland, das damit auf Rang sieben weltweit liegt.[3] Typische Angriffsmuster sind Phishing, Malware-Distribution, maliziöse Domains sowie Angriffe auf Telearbeit-Infrastrukturen (Remote-Zugriffe).

DER KLASSIKER: ERST VERSCHLÜSSELUNG DER DATEN, DANN LÖSEGELDFORDERUNG

Cyberangriffe auf Arztpraxen lohnen sich für die Täter doppelt: Nach einer Verschlüsselung der Praxis-EDV ist ein regulärer Praxisbetrieb meist nicht mehr möglich. Oft müssen die Geschädigten befürchten, dass womöglich hochsensible Patientendaten abgeflossen und in Täterhand gelangt sind. Nach einer erfolgreichen Verschlüsselung der Daten dauert es in der Regel nicht lange, bis die Täter per E-Mail eine Lösegeldforderung stellen. Neben dem Lösegeld für die Freigabe der Daten fordern sie mehr Geld dafür, dass sie die besonders geschützten Patientendaten nicht öffentlich machen. Ermittler nennen das „Double Extortion". Die Höhe der Summe variiert sehr stark und ist abhängig davon, wie die Täter die Liquidität des Opfers einschätzen. Die Forderungen können dabei vom niedrigen vierstelligen Bereich bis zum Millionenbetrag reichen.

WICHTIGER RAT: MITARBEITER SCHULEN UND EINE GESUNDE SKEPSIS

Viele Ärztinnen und Ärzte sind mit der Führung ihrer Praxis voll ausgelastet. In Sachen Computertechnik greifen sie häufig auf IT-Dienstleister zurück. Diese

[2] DDoS: Distributed Denial of Service
[3] https://www.mcafee.com/enterprise/en-us/lp/covid-19-dashboard.html, Abruf: 28.10.2020, 13:40 Uhr

kümmern sich nicht nur um die IT-Struktur, sondern auch um den Internetauftritt der Praxis. Das spart Zeit und ist praktisch, hat jedoch einen Nachteil: Häufig sorgt der Einsatz von IT-Dienstleistern dafür, dass man sich selbst mit der Materie nicht mehr beschäftigt. Man verlässt sich auf das Know-how des Serviceanbieters und hofft, damit gegen alle Tücken gefeit zu sein. Doch so gut der Dienstleister auch sein mag – es gibt immer noch Bereiche der IT-Sicherheit, die von allen Praxismitarbeiterinnen und -mitarbeitern beherzigt werden müssen. Es ist daher ratsam, Mitarbeiterinnen und Mitarbeiter in zeitlichen Abständen immer wieder für die bestehenden Gefahren zu sensibilisieren und entsprechend zu schulen. Das Wissen, welche Taten geschehen können und wie Täterinnen und Täter vorgehen, ist bei der Verhinderung von Cyberangriffen enorm wichtig. Geschultes Personal kann die Praxis vor einem großen finanziellen Schaden bewahren.

Kenntnisse über die Wichtigkeit von Datensicherung, Passwörtern und Softwareaktualisierung sowie Phishing-Mails sind in der Regel nicht hochtechnisch belastet und können somit schnell verinnerlicht werden. Hilfreich ist auch, ein Szenario für die eigene Praxis durchzuspielen, wie es weitergeht, wenn es doch zu einem Angriff von Cyberkriminellen kommen sollte. Damit deckt man eventuell vorhandene Sicherheitslücken auf und kann bestimmte Regeln für die eigene Praxis aufstellen.

Dirk Hintermeier ist Landeskoordinator Prävention Cybercrime bei der Zentralstelle Kriminal- und Verkehrsprävention beim Hessischen Landeskriminalamt in Wiesbaden.

GEFAHREN WERDEN BELEUCHTET

In den kommenden Ausgaben von Auf den PUNKT. werden die KV Hessen und das Hessische Landeskriminalamt mögliche Gefahrenquellen noch näher beleuchten. Wir freuen uns auf Anregungen und Fragen aus der Leserschaft. ■

Dirk Hintermeier

SIE HABEN FRAGEN?

Die Zentralstelle Kriminal- und Verkehrsprävention des Hessischen Landeskriminalamts hilft Ihnen gerne weiter.

E. Praeventioncybercrime@polizei.hessen.de

Infobox

Aktuelle Cyber-Attacken:

Robert-Koch-Institut (RKI): Cyberkriminelle haben am 22. Oktober 2020 die Webseite des RKI zeitweise durch einen sogenannten DDoS-Angriff lahmgelegt. Der Angriff erfolgte morgens zwischen 8.00 und 10.00 Uhr.

Uniklinik Düsseldorf: Unbekannte Hacker haben offenbar bereits Anfang 2020 ein Schadprogramm in das System der Uniklinik eingeschleust: Verschlüsselt wurden die Server des Klinikums am frühen Morgen des 10. September 2020. Daraufhin legte ein IT-Ausfall die Notaufnahme lahm. Eine Patientin starb, nachdem ihr Rettungswagen in eine weiter entfernte Klinik umgeleitet werden musste.