ZG_OBERGERICHT BS 2022 2 vom 28. September 2022

ZG Obergericht, 2022-09-28, DE

Quelle: https://mcp.opencaselaw.ch/entscheid/zg_obergericht_BS_2022_2

FR: ZG_OBERGERICHT BS 2022 2 du 28 septembre 2022

IT: ZG_OBERGERICHT BS 2022 2 del 28 settembre 2022

Regeste

I. Beschwerdeabteilung

Erwägungen

E. 1

Die Staatsanwaltschaft begründete die Einstellung des Verfahrens zusammengefasst wie folgt (act. 1/3):

E. 1.1

Der Beschuldigte habe sich nicht der unbefugten Datenbeschaffung (Art. 143 StGB) strafbar gemacht. Er habe sich anlässlich der Hausdurchsuchung spontan dahingehend geäussert, dass er von den Kunden der Beschwerdeführerin den Auftrag erhalten habe, deren Daten in ein anderes System zu überführen, da die Beschwerdeführerin die Herausgabe der Daten verweigert habe. Die jeweiligen Kunden hätten sich aber selbständig in die Systeme der Beschwerdeführerin eingeloggt und dem Beschuldigten anschliessend die Kontrolle über die Systeme überlassen, damit dieser die Daten der Kunden habe herunterladen können. Dieses Vorgehen sei von den Zeugen anlässlich der Einvernahme bestätigt worden. Die Kunden hätten wechseln wollen und die Beschwerdeführerin die Datenherausgabe teilweise verweigert, weshalb sich die Zeugen gezwungen gesehen hätten, mithilfe des Beschuldigten mit ihren Logins die Daten zu migrieren.

E. 1.2

Der Beschuldigte habe sich auch nicht des unbefugten Eindringens in ein Datenverarbeitungssystem (Art. 143bis StGB) strafbar gemacht. Alle Zeugen hätten übereinstimmend ausgesagt, dem Beschuldigten ihre Passwörter nicht überlassen zu haben. Seien solche benötigt worden, hätten die Zeugen diese selbst eingegeben. Der Beschuldigte habe zu keiner Zeit irgendeine elektronische Sicherung der Beschwerdeführerin umgangen und damit nicht irgendwelche Zugangsschranken überwunden. Die Aussagen des Beschuldigten und der Zeugen zeigten klar auf, dass weder der Beschuldigte noch eine andere Person aus dem Umfeld der A._____ GmbH in das System der Beschwerdeführerin im Sinne des Tatbestandes eingedrungen sei. Der Beschuldigte habe die Zeugen einzig bei ihrem Wechsel auf die Systeme der A._____ GmbH unterstützt.

E. 1.3

Auch des unbefugten Beschaffens von Personendaten (Art. 179novies StGB) habe sich der Beschuldigte nicht strafbar gemacht. Der Beschuldigte habe keine Daten der Beschwerdeführerin beschafft. Die Personendaten gehörten einzig den Zeugen, welche

 diese Daten auf das System der A._____ GmbH hätten übertragen wissen wollen. Hierfür habe weder der Beschuldigte noch eine andere Drittperson

Sicherungsmechanismen oder Zugangssperren überwinden müssen.

E. 1.4

Die Untersuchungen hätten sodann auch keine Hinweise auf ein sonstiges strafbares Verhalten ergeben. Die Zeugen hätten klar ausgesagt, sie seien mit den Leistungen der Beschwerdeführerin nicht mehr zufrieden gewesen und hätten deshalb den Anbieter gewechselt. Hingegen gebe es keinen hinreichenden Verdacht, dass die in der Anzeige und den Ergänzungen geschilderten Probleme der Beschwerdeführerin auf das Mitwirken des Beschuldigten bei der Datenmigration zurückzuführen seien. Die angebliche zeitliche Konnexität zwischen den Problemen der Beschwerdeführerin und der Unterstützung des Beschuldigten bei der Datenmigration würden keinen hinreichenden Verdacht für eine strafbare Handlung darstellen. Eine weitere Strafuntersuchung würde somit einer unerlaubten "fishing expedition" gleichkommen. Bezüglich der bereits in den Verfahren 2A 2017 2-4 abgehandelten Sachverhaltskomplexe (Strafanzeige vom 23. Dezember 2016 u.a. gegen den Beschuldigten bezüglich Kopierens und Verwendens des Sourcecodes der Beschwerdeführerin, Abwerben von Kunden) greife sodann der Grundsatz "ne bis in idem", weshalb diesbezüglich ein Verfahrenshindernis bestehe.

E. 2

Die Beschwerdeführerin rügt in ihrer Beschwerde zusammengefasst Folgendes:

E. 2.1

Vorliegend gehe es bei den Aktivitäten des Beschuldigten nicht bloss um das Herunterladen der Daten von – ihn angeblich autorisierenden – Kunden, sondern es hätten bewiesenermassen weitergehende Eingriffe in das besonders geschützte IT-Gesamtsystem der Beschwerdeführerin stattgefunden. Der Beschuldigte habe an den internen IT-Systemen und Datenbanken der Beschwerdeführerin sowie an fremden Kundendaten nachweislich strafrechtlich relevante Manipulationen vorgenommen durch a) weitergehende Informationsbeschaffungen aus den IT-Systemen der Beschwerdeführerin, b) Beschaffung von Daten unbeteiligter Drittkunden und c) Implementierung von fremden Programmcodes auf den IT-Systemen der Beschwerdeführerin. Dieses Vorgehen könne nicht durch irgendwelche Kundeneinwilligungen legitimiert werden, weil diese auch nicht involvierte Kunden sowie die Informatiksysteme der Beschwerdeführerin beträfen.

E. 2.2

Der Beschuldigte habe sich dabei weitergehende Informationen aus den Systemen der Beschwerdeführerin beschafft, als dies über das Kundenlogin möglich sei. Der Account bzw. Login der Kunden umfasse einzig die Zugangs- und Nutzungsberechtigungen der Applikationen der Beschwerdeführerin, wodurch Funktionen der Applikation genutzt sowie Patientendaten bewirtschaftet und verwaltet werden könnten. Systemtechnisch sei ein direktes Herunterladen der Kundendaten hingegen nicht möglich und es bestehe technisch keine Möglichkeit, direkt auf die Systeme und insbesondere auf die Datenbanken mit den Patientendaten zuzugreifen, um daraus Datenextrakte für Kunden zu erstellen. Hierfür seien vielmehr zusätzliche, illegale System- und Programmmanipulationen ("Upload-Backup-Programme") notwendig, wie sie im Forensikbericht vom 30. Oktober 2020 dokumentiert und nachgewiesen seien. Nach dem Programm-Update zu Beginn des Jahres 2020 sei es dem Beschuldigten nicht mehr möglich gewesen, im gewohnten Umfang und mit dem eingespielten Vorgehen an die Datenbank mit den Kundendaten zu gelangen. Er habe

Seite 7/12 deshalb das Berechtigungssystem des Servers der Beschwerdeführerin mit Hackingtools "aushebeln" müssen, wie dies im Forensikbericht vom 30. Oktober 2020 bewiesen werde. Hierbei sei das System der Beschwerdeführerin im bestimmungsgemässen Betrieb gestört und schlussendlich jeweils auch in erheblichem Umfang beschädigt zurückgelassen worden. Das Vorgehen des Beschuldigten könne deshalb nicht mit der Einwilligung der Kunden, ihre Daten zu extrahieren oder ihre Account- und Passwortdaten bereitzustellen, begründet werden. Die entsprechenden Ausführungen in der Einstellungsverfügung seien ein technischer und juristischer Fehlschluss.

E. 2.3

Der Beschuldigte sei sodann nachgewiesenermassen in die interne IT-Systeminfrastruktur der Beschwerdeführerin eingedrungen.

E. 2.3.1

Aus dem Forensikbericht vom 30. Oktober 2020 ergebe sich aus Ziff. 2.2.4 beispielsweise, dass der Beschuldigte mit den Logindaten von N._____ (dessen Einwilligung nicht vorliege) auf den Account von N._____ und nach der Überwindung zusätzlicher Sicherheitsbarrieren widerrechtlich auf die internen IT-Systembereiche der Beschwerdeführerin (Entwicklungsumgebung, Kundenverwaltung) zugegriffen habe. Um diese Sicherheitsschranken zu durchbrechen, habe der Beschuldigte nachgewiesenermassen diverse Administratoren-Passwörter vom internen Domänen- Controlling der Beschwerdeführerin ausprobiert. Gleichzeitig habe der Beschuldigte die Benutzernamen und Passwörter eines ehemaligen Entwicklers der Beschwerdeführerin eingesetzt und ausprobiert sowie diejenigen eines aktuell angestellten Entwicklers missbraucht. Diese Angriffe seien in mehreren Fällen erfolgreich gewesen. So habe der Beschuldigte mit den Userdaten von O._____ ("___.Station1") die erste Sicherheitshürde überwinden und über den Server TS52 auf die internen IT-Systeme der Beschwerdeführerin zugreifen können, z.B. die interne Kundenverwaltung, Buchhaltung, Entwicklungsumgebung und die neueren Versionen der Software. Dazu habe der Beschuldigte von der Domäne "B._____" aus die Benutzeradministratoren "__" und "__" verwendet (Forensikbericht vom 30. Oktober 2020, Ziff. 2.2.5). Der Administrator "__" habe dabei keinen Zugang zu Kundendaten, sondern beschäftige sich mit der Kundenverwaltung und Source-Code-Arbeiten. Die missbräuchlich verwendete Benutzer-ID "__" könne somit keinesfalls für die Beschaffung von Kundendaten verwendet worden sein. Dafür habe der Beschuldigte diverse Sicherheitsschranken überwinden müssen, wobei er auch auf die Terminalserver TS_, TS_, TS_ und TS_ zugegriffen habe. Auf diesen Servern werde eine Vielzahl anderer Kunden gehostet. Aus dem Forensikbericht vom 30. Oktober 2020 ergebe sich zudem, dass sich der Beschuldigte auf den internen Server "___-01" mit RDP und in das SQL-Server-Management mit "Administrator" eingeloggt habe. Hierfür habe er sich mit einem speziellen Passwort einloggen müssen, welches nur den Entwicklern der Beschwerdeführerin bekannt sei. Der Administrator "___-01" habe dabei Zugriff auf tausende versendete Rechnungen der Beschwerdeführerin, nicht jedoch auf Kundendaten, weshalb auch dieser Zugriff keinesfalls durch Kundeneinwilligung legitimierbar sei. Die Datenbank-Server seien vom Internet aus nicht erreichbar, weshalb der Beschuldigte Logindaten von Kunden habe missbrauchen müssen, um die erste Sicherheitshürde des Servers TS_ zu umgehen. Sodann habe er sich interne Administratorenpasswörter der

Seite 8/12 Beschwerdeführerin beschaffen und diese verwenden müssen, um widerrechtlichen Zugang zu diesen Bereichen zu erlangen. Die Staatsanwaltschaft ignoriere diese Fakten vollständig. Die Einwilligung zum Download von Kundendaten hätten mit diesen nachweislich festgestellten kriminellen Tätigkeiten des Beschuldigten nichts mehr zu tun.

E. 2.3.2

Der Beschuldigte habe ausserdem Angriffe auf andere Anwenderkonten verübt. Unter Verwendung des Benutzernamens und der Zugangsdaten des Zeugen P._____ seien Angriffe auf andere Anwenderkonten im System der Beschwerdeführerin durchgeführt worden, welche nicht von einer Einwilligung der Kunden gedeckt sein könnten. Dabei sei die Systemumgebung des Accounts des Zeugen P._____ derart stark beschädigt worden, dass die Systemumgebung nicht mehr bestimmungsgemäss ausführbar gewesen sei. Im Forensikbericht vom 30. Oktober 2020 seien Start- und Endzeiten der einzelnen Zugriffe auf Kundendaten nicht einwilligender Kunden dokumentiert (vgl. act. 1 S. 15 f.). Teilweise habe sich der Beschuldigte von diesen Kundenaccounts aus auf Systeme anderer Kunden weiterverbunden.

E. 2.3.3

Der Beschuldigte habe zudem auf Kundendaten von nicht beteiligten Drittkunden, welche keinen Auftrag für eine Datenextraktion erteilt hätten, zugegriffen und diese weiterverwendet. Gemäss Forensikbericht vom 30. Oktober 2020 habe der Beschuldigte zuerst über Kundenlogins versucht, auf weitere Kundendaten zuzugreifen und sich wenig später mit den Kundendaten dieser unbeteiligten Drittkunden angemeldet. Am 13. Oktober 2020 habe sich der Beschuldigte beispielsweise mit dem Usernahmen von Q._____ ohne dessen Einwilligung eingeloggt und wiederholt auf das System der Beschwerdeführerin zuzugreifen versucht (vgl. act. 1 S. 18 f.). Dabei sei es dem Beschuldigten gelungen, auf Server zuzugreifen, welche hochsensible Rechnungsdaten und Mails der Beschwerdeführerin enthielten. Auf diese Server habe kein Kunde Zugriff und diese seien vom Internet aus nicht erreichbar. Der Beschuldigte habe somit Kundenlogins missbrauchen müssen, um die erste Sicherheitshürde zum Terminalserver TS_ überwinden zu können. Sodann habe er sich mit internen Administratorenpasswörtern der Beschwerdeführerin auf die internen Systeme weiterverbunden.

E. 2.3.4

Überdies habe sich der Beschuldigte nachweislich im Oktober 2020 mit den Benutzerdaten von R._____, Mitarbeiter der Beschwerdeführerin, angemeldet und sodann am 22. und 23. Oktober 2020 auf den Server "___01" zugegriffen, welcher über die Kundendomäne nicht erreichbar sei. Darauf seien die interne Kundenverwaltung, die Buchhaltung der Beschwerdeführerin, Störungsmeldungen und E-Mails der Kunden abgelegt. Die Login-Informationen würden von R._____ mit niemandem geteilt, weshalb der Beschuldigte diese aus den internen Systemen der Beschwerdeführerin beschafft haben müsse. Diese Zugriffe auf das interne System der Beschwerdeführerin würden in der Einstellungsverfügung nicht abgehandelt, sondern schlicht totgeschwiegen.

E. 2.4

Der Beschuldigte habe schliesslich eigene Programme in die Systemumgebung der Beschwerdeführerin implementiert. Die entsprechende Auflistung ergebe sich aus dem Forensikbericht vom 30. Oktober 2020 auf den Seiten 17-25. So habe der Beschuldigte das

von ihm entwickelte Programm "UploadBackup.exe" mindestens auf den Servern TS_, TS_ und TS_ der Beschwerdeführerin ausgeführt. Am 9. Oktober 2020 habe der Beschuldigte versucht, mit dem "SQL Server Management Studio" und dem Taskmanager innerhalb einer

Seite 9/12 Remote-Desktop-Sitzung Anmeldeinformationen auszulesen. Am 23. Oktober 2020 habe der Beschuldigte eine RDP-Sitzung von TS_ auf "___01" aufgebaut und ein Programm geöffnet, mittels welchem er Zugangsdaten der Kunden erhalten habe. Mit dem selbst entwickelten Programm "UploaderBackup.exe" habe der Beschuldigte Kundendaten unbeteiligter Dritter gesammelt und herauskopiert. Auch damit setze sich die Staatsanwaltschaft in der Einstellungsverfügung nicht auseinander.

E. 3

Die Staatsanwaltschaft verfügt gemäss Art. 319 Abs. 1 StPO unter anderem dann die Einstellung des Verfahrens, wenn kein Tatverdacht erhärtet ist, der eine Anklage rechtfertigt (lit. a), wenn kein Straftatbestand erfüllt ist (lit. b) oder wenn Rechtfertigungsgründe einen Straftatbestand unanwendbar machen (lit. c). Der Entscheid über die Einstellung eines Verfahrens hat sich nach dem Grundsatz "in dubio pro duriore" zu richten. Danach darf eine Einstellung durch die Staatsanwaltschaft grundsätzlich nur bei klarer Straflosigkeit oder offensichtlich fehlenden Prozessvoraussetzungen angeordnet werden. Hingegen ist, sofern die Erledigung mit einem Strafbefehl nicht in Frage kommt, Anklage zu erheben, wenn eine Verurteilung wahrscheinlicher erscheint als ein Freispruch. Ist ein Freispruch genauso wahrscheinlich wie eine Verurteilung, drängt sich in der Regel, insbesondere bei schweren Delikten, eine Anklageerhebung auf. Bei zweifelhafter Beweis- oder Rechtslage hat nicht die Staatsanwaltschaft über die Stichhaltigkeit des strafrechtlichen Vorwurfs zu entscheiden, sondern das zur materiellen Beurteilung zuständige Gericht. Der Grundsatz, dass im Zweifel nicht eingestellt werden darf, ist auch bei der Überprüfung von Einstellungsverfügungen zu beachten (BGE 143 IV 241 E. 2.2 m.w.H.).

E. 4

Die Staatsanwaltschaft stützt ihre rechtliche Würdigung in der Einstellungsverfügung auf eine Sachverhaltsfeststellung, welche sich nicht in dieser Klarheit aus den Akten ergibt.

E. 4.1

So geht die Staatsanwaltschaft davon aus, der Beschuldigte habe zu keiner Zeit irgendeine elektronische Sicherung der Beschwerdeführerin umgangen und sei abgesehen vom Kundenlogin nicht in das System der Beschwerdeführerin eingedrungen. Er habe die Zeugen einzig bei ihrem Wechsel auf die Systeme der A._____ GmbH unterstützt, indem er ihre Daten mithilfe ihres Logins extrahiert habe. Hingegen nimmt die Staatsanwaltschaft keine Stellung zu den Behauptungen der Beschwerdeführerin, dass (1) der Beschuldigte – neben der Migration von Daten seiner neuen Kunden – auf Daten unbeteiligter Kunden zugegriffen und diese eventuell kopiert habe, (2) er in das System der Beschwerdeführerin eingedrungen sei und (3) hierfür Login-Daten von unbeteiligten Kunden sowie Mitarbeitenden der Beschwerdeführerin verwendet habe, (4) dass der Beschuldigte eigene Programme auf dem System der Beschwerdeführerin installiert, verwendet und wieder gelöscht und (5) weitergehende Informationen aus den Systemen der Beschwerdeführerin beschafft habe, als dies über das Kundenlogin möglich sei. Die Beschwerdeführerin trug ihre Behauptungen dabei substanziiert vor und verwies auf

entsprechende Beweismittel. Aus den Akten ergeben sich dennoch keine Hinweise, dass die Staatsanwaltschaft die Behauptungen der Beschwerdeführerin geprüft hätte.

E. 4.2

Vielmehr stützt sich die Staatsanwaltschaft bei ihren Sachverhaltsfeststellungen einzig auf die Aussagen der vier Zeugen sowie eine spontane Äusserung des Beschuldigten anlässlich der Hausdurchsuchung. Dabei fällt auf, dass keiner der Zeugen darlegen konnte, wie der Beschuldigte an die Kundendaten gelangte, obwohl die Zeugen selbst die Daten nicht

Seite 10/12 extrahieren konnten. Auch konnten die Zeugen nicht nachvollziehen, was der Beschuldigte im Rahmen der Datenmigration mithilfe ihres Accounts tat. Der Beschuldigte selbst wurde nicht dazu befragt, wie er die Datenmigration genau gestaltete, insbesondere als diese nicht reibungslos funktionierte.

E. 4.3

Die Beschwerdeführerin ihrerseits legte einen Forensikbericht der G._____ AG (Vi act. D 4/1/5) vor, der ihrer Darstellung der geschilderten Vorgänge zugrunde liegt, und beschreibt unter Verweis auf diesen Bericht detailliert, welche Handlungen an welchem Datum durch eine Person mit der IP-Adresse des Beschuldigten vorgenommen worden seien. Die Staatsanwaltschaft erklärt nicht, weshalb der Forensikbericht und die daraus abgeleiteten Schlussfolgerungen der Beschwerdeführerin unzutreffend sein sollen. Es ist somit nicht ersichtlich, wie die Staatsanwaltschaft zu ihrer abweichenden Sachverhaltsfeststellung gelangt. Aufgrund des Forensikberichts vom 30. Juni 2020 und den detaillierten, mit objektiven Beweismitteln zumindest plausibel dargelegten Behauptungen der Beschwerdeführerin ist der Sachverhalt somit nicht genügend geklärt, um gestützt darauf das Strafverfahren gegen den Beschuldigten einzustellen.

E. 4.4

Der von der Beschwerdeführerin behauptete Sachverhalt würde sodann ein strafbares Verhalten des Beschuldigten nahelegen. Dieses wäre insbesondere nicht durch die Einwilligung bestimmter Kunden gerechtfertigt, da gemäss Darstellung der Beschwerdeführerin ihre eigenen IT-Systeme und unbeteiligte Drittkunden betroffen gewesen seien. Auf weitergehende Ermittlungen kann deshalb auch nicht aufgrund einer antizipierten Beweiswürdigung verzichtet werden.

E. 5

Die Beschwerde ist somit gutzuheissen, die Einstellungsverfügung vom 29. Dezember 2021 aufzuheben und das Verfahren zur weiteren Abklärung an die Staatsanwaltschaft zurückzuweisen.

E. 5.1

Die Staatsanwaltschaft ersuchte für diesen Fall das Obergericht, die Sachverhaltskomplexe, die weiter zu untersuchen sind, zu bezeichnen. Aufgrund der Vorbringen der Beschwerdeführerin (vorne E. 3) wird namentlich abzuklären sein, ob der Beschuldigte i) weitergehende Informationen oder Daten aus den Systemen der Beschwerdeführerin beschaffte, als dies über das Kundenlogin möglich war, ii) ob er in die interne IT-Systeminfrastruktur der Beschwerdeführerin eingedrungen ist, iii) ob er dadurch Kundendaten oder andere Informationen erlangte und iv) ob er Programme in die Systemumgebung der Beschwerdeführerin implementierte. Dabei wird zu klären sein, ob

die in diesem Zusammenhang gemachten Feststellungen im Forensikbericht vom 30. Oktober 2020 und die daraus gezogenen Schlüsse der Beschwerdeführerin zutreffend sind.

E. 5.2

Hingegen erscheint eine Abklärung des Sachverhalts, welcher der Nichtanhandnahmeverfügung vom 21. Februar 2017 in den Verfahren 2A 2017 2-4 zugrunde lag, nicht angezeigt. Dies wird von der Beschwerdeführerin im Beschwerdeverfahren auch nicht geltend gemacht. Inwieweit Abklärungen zu Störungen der Systemumgebung der Beschwerdeführerin vorzunehmen sind, kann beim aktuellen Ermittlungsstand nicht beurteilt werden. Hierfür ist insbesondere relevant, ob sich die von der Beschwerdeführerin behaupteten Aktivitäten des Beschuldigten so zugetragen haben und ob diese geeignet wären, die behaupteten Störungen zu verursachen.

E. 5.3

Schliesslich wird die Staatsanwaltschaft in einem hinreichend begründeten Entscheid über das Gesuch der Beschwerdeführerin um Einsicht in die Akten der Nebendossiers 1 und 2 zu entscheiden haben. Wie die Beschwerdeführerin in der Beschwerde zutreffend rügt, hat die Staatsanwaltschaft bisher keine begründete Verfügung erlassen, in welcher sie – unter Hinweis auf die gesetzlichen Anforderungen der Einschränkung der Akteneinsicht – ihren ablehnenden Entscheid näher begründet. Der Verweis auf die "Usanz", gewisse Teile der Untersuchungsakten nicht zur Verfügung zu stellen, erfüllt die Anforderung an die Begründung der Einschränkung des Akteneinsichtsrechts nicht.

E. 6

Hebt die Beschwerdeinstanz einen Entscheid auf und weist die Sache an die Vorinstanz zurück, sind die Kosten des Beschwerdeverfahrens auf die Staatskasse zu nehmen (Art. 428 Abs. 4 StPO). Die Beschwerdeführerin ist zudem für die notwendigen Aufwendungen im Beschwerdeverfahren aus der Staatskasse zu entschädigen (Art. 436 Abs. 3 StPO; Schmid/ Jositsch, Schweizerische Strafprozessordnung, Praxiskommentar, 3. A. 2018, Art. 436 StPO N 4; Wehrenberg/Bernhard, Basler Kommentar, 2. A. 2014, Art. 436 StPO N 8; je m.H.).
Beschluss