ZG_OBERGERICHT BS 2025 4 vom 6. Juni 2025

ZG Obergericht, 2025-06-06, DE

Quelle: https://mcp.opencaselaw.ch/entscheid/zg_obergericht_BS_2025_4

FR: ZG_OBERGERICHT BS 2025 4 du 6 juin 2025

IT: ZG_OBERGERICHT BS 2025 4 del 6 giugno 2025

Regeste

I. Beschwerdeabteilung

Erwägungen

E. 1

Gegen Entscheide der Staatsanwaltschaft kann innert 10 Tagen bei der I. Beschwerdeabteilung des Obergerichts Beschwerde geführt werden (Art. 20 Abs. 1 lit. b StPO, Art. 393 Abs. 1 lit. a StPO, Art. 396 Abs. 1 StPO, § 21 Abs. 1 Bst. b GOG und § 7 Abs. 1 GO OG). Auf die unbestrittenermassen frist- und formgerecht eingereichte Beschwerde der Beschwerdeführe- rin vom 16. Januar 2025 ist grundsätzlich einzutreten. Mit der Beschwerde können Rechtsverletzungen, die unvollständige oder unrichtige Sachverhaltsfeststellung und die Unangemessenheit gerügt werden (Art. 393 Abs. 2 StPO). Die Beschwerdeinstanz entscheidet in einem schriftlichen Verfahren (Art. 397 Abs. 1 StPO). Sie verfügt über volle Kognition (Art. 391 Abs. 1 StPO).

E. 2

Die Staatsanwaltschaft begründet die Einstellung des Untersuchungsverfahrens zusammengefasst wie folgt:

E. 2.1

Die Beschwerdeführerin habe für die Datenanalyse und -sammlung die externe Firma K._____ AG beigezogen. Diese habe für den Auftrag das Client-Server-Programm AC._____ eingesetzt. Ein solches Tool könne zur Überwachung und Analyse von Syste- men grosser IT-Umgebungen eingesetzt werden. Es sei fraglich, ob die durch den Einsatz des Programmes AC._____ gewonnenen Erkenntnisse als zulässige Beweismittel anzu- sehen seien. Beweismittel seien nur verwertbar, wenn sie durch die Strafverfolgungsbehör- den auf diese Art und Weise rechtmässig erlangt hätten werden können (Art. 141 Abs. 2 StPO). Unabhängig davon, ob die durch den Einsatz des Programmes gewonnenen Er- kenntnisse als zulässige Beweismittel anzusehen seien, sei das Untersuchungsverfahren gegen den Beschuldigten jedoch einzustellen.

E. 2.2

Der Ersteller des AD._____ Report, V._____, habe an der Zeugenbefragung nicht sagen können, wie die IP-Adresse R._____ gefunden worden sei, auf welche im Report Bezug genommen werde. Diese sei der K._____ AG von der Beschwerdeführerin so mit- geteilt worden, da sie als ungewöhnlich aufgefallen sei. Wie genau die Beschwerdeführerin auf diese IP-Adresse gekommen sei, habe der Zeuge nicht sagen können. Des Weiteren ha- be er erklärt, dass er nie eine Sicht auf die Firewall gehabt habe. Ihm sei von der Beschwer- deführerin gesagt worden, dass "komische Sachen" festgestellt

worden seien und man des- halb auf die Firewall geschaut und dort die IP-Adresse gesehen habe. Auch der Beschuldigte habe bereits im Schreiben vom 15. Dezember 2022 festgestellt, dass der Bericht der K._____ AG sich darüber ausschweige, woher die öffentliche IP-Adresse R._____ stamme und wieso gerade diese dem angeblichen Angreifer gehören solle. In diesem Zu- sammenhang habe der Beschuldigte auf weitere Ungereimtheiten hingewiesen: So seien gemäss Bericht der K._____ AG die meisten Zugriffe über die Kundengeräte erfolgt. In diesem Fall hätte die IP-Adresse R._____ keinesfalls geloggt werden können, da für das System der Zugriff vom Kundengerät erfolgt sei und somit von einem Dritten.

E. 2.3

DDos-Attacken seien von der K._____ AG gemäss dem Zeugen V._____ keine analysiert worden, da es hierzu keine Evidenzen gegeben habe und dies entsprechend auch

 nicht habe festgestellt werden können. Es habe keine Beweise gegeben, die dies erhärtet hätten.

E. 2.4

Der Zeuge habe des Weiteren in Bezug auf das Thema "laterale Bewegungen" angegeben, dass keine internen Sicherheitsschranken bei den lateralen Bewegungen hätten überwunden werden müssen; alles sei offen gewesen. Der Tatbestand von Art. 143 StGB verlange aber – so die Staatsanwaltschaft – dass die Daten gegen den unbefugten Zugriff des konkreten Täters besonders gesichert sein müssten. Somit erfüllten die zwei erfolgreichen lateralen Bewegungen, welche es gemäss AD._____ Report in den Systemen der Beschwerdeführ- rerin gegeben habe, den Tatbestand von Art. 143 StGB nicht. Darüber hinaus habe der Zeu- ge ausgeführt, dass er nicht nachweisen könne, was dort genau gemacht worden sei.

E. 2.5

Zum Thema Datenabfluss habe der Zeuge angegeben, dass er keine Firewall-Logs habe, welche besagten, dass Daten hinausgeflossen seien. Somit gebe es, so die Staatsanwaltschaft, offensichtlich keine Anzeichen dafür, dass Daten aus dem Netzwerk oder aus dem System der Beschwerdeführerin nach aussen gelangt seien. Das Fehlen von Logs bedeute zwar nicht zwangsläufig, dass kein Datenabfluss stattgefunden habe. Da Spuren in technischer Hinsicht fehlten, liessen sich auch keine weiteren Aussagen dahingehend machen, die auf ein strafbares Verhalten des Beschuldigten und/oder einer erweiterten Täterschaft im Zu- sammenhang mit dem Datenabfluss hinweisen würden.

E. 2.6

Der AD._____ Report enthalte eine Übersicht über die Zugriffe. Der Zeuge V._____ sei gefragt worden, wie er sich erklären könne, dass bei einem Angreifer überschneidende und gleichzeitige Remote-Desktop-Sitzungen möglich gewesen sein sollen. Der Zeuge habe eingestehen müssen, dass es ein Fehler sein müsse. Sei es der gleiche Benutzer, dann sei es nicht möglich, dass gleichzeitig zwei Sessions stattfinden könnten. Auch beim Zugriff auf die Systeme der Beschwerdeführerin via O._____ habe der Zeuge bestätigt, dass dies auf Annahmen basieren würde. Sodann habe der Zeuge ausgesagt, dass die beiden Tools AN._____ und AO._____ nur zum Angriff, nicht aber zum Eindringen in das System der Beschwerdeführerin verwendet worden seien.

E. 2.7

Gestützt auf die Aussagen des Zeugen V._____ habe festgestellt werden müssen, dass der Report der K._____ AG in einigen Punkten nicht korrekt sei und Unstimmigkeiten aufweise. Zudem habe sich aus den Aussagen des Zeugen ergeben, dass bei der Erstellung des Reports von Annahmen ausgegangen worden sei.

E. 2.8

Die in der Strafanzeige formulierten Vorwürfe hätten ihre Grundlage im Bericht der K._____ AG, einem (Privat-)Gutachten, das auf Daten basiere, welche mit dem Programm AC._____ erhoben worden seien. Gestützt auf die Strafanzeige und den AD._____ Report seien anlässlich der diversen Triage-Verhandlungen unter der Leitung des Zwangsmassnahmengerichts die sichergestellten Systeme des Beschuldigten/der H._____ GmbH mit Stichworten durchsucht worden. Mit den vom Zwangsmassnahmen- gericht letztlich freigegebenen Daten und Unterlagen hätten die in der Strafanzeige formulier- ten Vorwürfe jedoch nicht bewiesen bzw. erhärtet werden können.

E. 2.9

Die Beschwerdeführerin sei mit Schreiben vom 10. August 2023 ersucht worden, die Ziel-IP- Adresse im Zusammenhang mit dem vorliegenden Strafverfahren bekannt zu geben. Die Be-

Seite 10/20 schwerdeführerin habe in der Folge verschiedene interne und externe IP-Adressen übermit- telt. In der Folge sei die Zuger Polizei, Dienst IT Forensik, vom Zwangsmassnahmengericht beauftragt worden, in den aufbereiteten Daten, welche im Bericht zur forensischen Datenauf- bereitung vom 15. Juni 2023 dokumentiert seien, jeweils nach den ersten drei Oktetten der AE._____-Adressen (AF._____ und AG._____) zu suchen. Die Ermittlungen der Zuger Polizei hätten ergeben, dass eine Ermittlung der Täterschaft einzig aufgrund von loka- len IP-Adressen von Terminalservern und den zur Verfügung stehenden Daten nicht möglich sei. Die Einschätzung der Staatsanwaltschaft, wonach die von der Beschwerdeführerin gel- tend gemachten lokalen (internen) AE._____-Adressen vernachlässigt werden könnten, da diese nicht zur Ermittlung der Täterschaft führen würden, sei somit zutreffend gewesen.

E. 2.10

Die Abklärungen zu den Event-Logs hätten ebenfalls zu keinen Hinweisen geführt, welche eine Tatbegehung des Beschuldigten belegen würde. Entsiegelt worden sei ein WhatsApp-Chat mit der Kennung "AH._____ Der Zuger Polizei sei es nicht möglich gewesen, die Chatpartner etc. zu eruieren. Es habe ein Austausch über Datenmigration stattgefunden. Erwähnt worden sei, dass ein Zugang gesperrt worden sei. Es sei indes nicht festzustellen gewesen, um was für einen Zugang es sich dabei gehandelt habe. In der Nachricht werde festgehalten, dass die Beschwerdeführerin die Datenbank verschlüsselt habe, wobei das Passwort aber habe "herausgefunden" werden können. Um welche Datenbank es sich gehandelt habe, habe nicht ermittelt werden können. Weitere Ermittlungen dazu seien nicht möglich, dies auch vor dem Hintergrund, dass nur ein Teil des Chats durch das Zwangsmassnahmengericht entsiegelt worden sei.

E. 2.11

Die Beschwerdeabteilung des Obergerichts habe im Beschluss vom 28. September 2022 festgehalten, dass die Beschwerdeführerin ihren Schilderungen den Forensikbericht der K._____ AG zugrunde gelegt habe und sie unter Verweis auf diesen Bericht detailliert

beschreibe, welche Handlungen an welchem Datum durch eine Person mit der IP-Adresse des Beschuldigten vorgenommen worden seien. Die Staatsanwaltschaft erkläre nicht, weshalb der Forensikbericht und die daraus abgeleiteten Schlussfolgerungen der Beschwerdeführerin unzutreffend sein sollten. Die Staatsanwaltschaft habe den Ersteller des Forensikberichts, V._____, einvernom- men. Dabei habe festgestellt werden müssen, dass der Bericht Unstimmigkeiten aufweise. Die IP-Adresse des Beschuldigten sei nicht von der K._____ AG selbständig so festge- stellt worden, sondern sei ihr von der Beschwerdeführerin mitgeteilt worden. Dies wie auch alle anderen Unstimmigkeiten in diesem Forensikbericht, die nicht gefundenen Spuren in den Systemen des Beschuldigten wie auch die Zeugenaussagen von ehemaligen Kunden der Beschwerdeführerin, die mit grössten Schwierigkeiten zu H._____ GmbH hätten wech- seln können, hätten dazu geführt, dass das Strafverfahren gegen den Beschuldigten und/oder eine erweiterte Täterschaft gesamthaft einzustellen sei. Der mit dem Parteigutach- ten dargestellte Sachverhalt in der Strafanzeige habe mit den Ermittlungen so nicht festge- stellt werden können und könne somit dem Beschuldigten so auch nicht vorgeworfen wer- den. Schlüssige Beweise für den von der Beschwerdeführerin dargelegten Sachverhalt hät- ten nicht gefunden werden können.

E. 2.12

Es habe insgesamt nicht erstellt werden können, dass der Beschuldigte oder eine andere, erweiterte Täterschaft sich widerrechtlich Zugriff zu den Systemen der Beschwerdeführerin

Seite 11/20 verschafft habe, insbesondere dass der Beschuldigte und/oder eine unbekannte Täterschaft weitergehende Informationen oder Daten aus den Systemen der Beschwerdeführerin be- schafft habe, als dies über das Kundenlogin möglich sei. Ebenso wenig sei erstellt, dass der Beschuldigte oder eine unbekannte Täterschaft in die interne IT-Systeminfrastruktur der Be- schwerdeführerin eingedrungen sei, dadurch Kundendaten oder andere Informationen er- langt und Programme in die Systemumgebung der Beschwerdeführerin implementiert hätte.

E. 2.13

Die sowohl von der Beschwerdeführerin als auch vom Beschuldigten gestellten Beweisanträ- ge seien insgesamt abzuweisen, da sie am Ergebnis nichts zu ändern vermöchten.

E. 3

Die Beschwerdeführerin macht demgegenüber – zusammengefasst – Folgendes geltend:

E. 3.1

Die Staatsanwaltschaft habe die Vorwürfe gemäss Strafanzeige und damit den Tatverdacht immer noch nicht analysiert. Sie habe zwar weitere Untersuchungshandlungen durchgeführt, aber die massgebenden und von der Beschwerdeführerin bereits mit der Strafanzeige beige- brachten Beweismittel nicht geprüft. Die fehlende Prüfung zeige sich exemplarisch darin, dass die Staatsanwaltschaft die 33 Evidenzen des Forensikberichts nicht analysiert habe. Die Zuger Polizei habe diese offenbar mangels technischer Mittel nicht analysieren können, was nicht zulässig sei. Der Zeuge V._____ habe an der Befragung mehrfach auf die Veri- fizierung von Evidenzen hingewiesen, welche geprüft werden müssten. Auch bei weiteren Fragen habe der Zeuge auf weitere Prüfhandlungen und Abklärungen verwiesen. Aufgrund der umfangreichen Zeugenbefragung von rund acht

Stunden und der Tatsache, dass die fo- rensische Analyse des Zeugen rund eineinhalb Jahre vor dessen Befragung erfolgt sei, seien allfällig unvollständige oder nicht bis ins Detail stimmige mündliche Antworten des Zeugen nicht ungewöhnlich. Es sei daher notwendig, den Zeugen insbesondere zu den Ausführun- gen der Zuger Polizei in den Berichten 2023 und 2024 sowie zu den Beweisanträgen des Beschuldigten zu befragen.

E. 3.2

Die Staatsanwaltschaft habe ausserdem die Zuger Polizei anzuweisen, entweder selber oder mittels anderer forensischer Polizeiabteilungen die zur Verfügung gestellten Evidenzen fo- rensisch auszuwerten, allenfalls mit Hilfe von Spezial-Tools und unter Beizug der Forensik, zumal die Staatsanwaltschaft die Forensik zur Sachverhaltsabklärung faktisch nicht beigezo- gen habe. Die Staatsanwaltschaft habe nicht begründet, weshalb sie keine forensische Ab- klärung habe durchführen lassen. Somit sei der Forensikbericht offensichtlich nicht hinrei- chend berücksichtigt und geprüft worden, obwohl er relevante Evidenzen enthalte, die für den Fall von entscheidender Bedeutung seien.

E. 3.3

Es sei nicht ersichtlich, weshalb die Anwendung der von der K._____ AG verwendeten Software AC._____ für die Auswertung der Daten der Beschwerdeführerin nicht zulässig gewesen sein solle. Zudem sei nicht nachvollziehbar, weshalb die Staatsanwaltschaft das Argument der Nichtverwertbarkeit wegen Art. 141 StPO erstmals in der aktuellen Einstel- lungsverfügung vorbringe.

E. 3.4

Im Forensikbericht der K._____ AG vom 30. Oktober 2020 werde im Detail aufgezeigt, wie der Angreifer vorgegangen sei, welcher Mittel und Programme er sich bedient habe, in welche Systeminfrastruktur der Beschwerdeführerin er eingedrungen sei, welche Zugangs- hürden er habe überwinden müssen und welche Datenbanken er transferiert habe. Dabei

Seite 12/20 habe der Forensikbericht auf 33 Einzelbeweise/Daten (Evidenzen) verwiesen. Bei diesen Evidenzen handle es sich um Daten aus dem System der Beschwerdeführerin. Wie erwähnt, habe die Staatsanwaltschaft die Evidenzen zum Forensikbericht nicht analysiert. Eine aus- reichende Würdigung des Berichts und den Schlussfolgerungen sei in der Einstellungsverfü- gung aber nicht erfolgt. Die Staatsanwaltschaft habe sich darauf beschränkt, die entsiegelten Daten aus der Hausdurchsuchung auszuwerten und der Zuger Polizei dazu einen Auftrag zu erteilen. Eine umfassende und sorgfältige Auswertung des Forensikberichts wäre jedoch er- forderlich gewesen, um eine objektive und rechtlich fundierte Entscheidung zu treffen.

E. 3.5

Was die IP-Adresse R._____ betreffe, so spiele es keine Rolle, wie diese gefunden wor- den sei. Es handle sich dabei unbestrittenermassen um die IP-Adresse des Beschuldigten und der Forensikbericht zeige, dass diese IP-Adresse mehrfach im System der Beschwerde- führerin gefunden worden sei, auch auf der Firewall. Gemäss K._____ AG seien die meisten Zugriffe zwar über die Kundengeräte erfolgt. Dies bedeute aber, dass nicht alle Zu- griffe über die Kundengeräte erfolgt seien, sondern die übrigen über die Firewall.

E. 3.6

Entgegen der Auffassung der Staatsanwaltschaft habe die Täterschaft sehr wohl interne Sicherheitsschranken überwinden müssen, auch bei den lateralen Bewegungen. Sämtliche Daten seien mit Passwort und Benutzernamen geschützt gewesen. Den Akten lasse sich ausserdem entnehmen, dass zumindest ein Passwort der Beschwerdeführerin gehackt worden sei. Dazu komme ein Hinweis in der internen Kommunikation der Firma des Beschuldigten, der H._____ GmbH, zwischen der Ehefrau des Beschuldigten mit dem damaligen Mitar- beiter W._____, welcher ebenfalls für eine widerrechtliche Vorgehensweise spreche. Im Forensikbericht werde sodann dargelegt, wie der Beschuldigte (z.B. mit den Logindaten von AI._____, fremder Kunde ohne Bezug und Einwilligungserklärung gegenüber der Täter- schaft) auf den Account von AI._____ und nach der Überwindung zusätzlicher Sicher- heitsbarrieren widerrechtlich auf interne IT-Systeme der Beschwerdeführerin zugegriffen ha- be. Um die dort eingesetzten Sicherheitsschranken zu durchbrechen, habe der Beschuldigte nachgewiesenermassen diverse Administratoren-Passwörter vom internen Domänen- Controller der Beschwerdeführerin ausprobiert. Gleichzeitig habe er auch die Benutzernamen und Passwörter von einem ehemaligen Entwickler der Beschwerdeführerin eingesetzt und ausprobiert sowie auch diejenigen von einem aktuell bei der Beschwerdeführerin angestell- ten Entwickler missbraucht. Der Beschuldigte habe somit mehrere Sicherheitsschranken durchbrechen müssen. Wie aus dem Forensikbericht ersichtlich, seien diese Angriffe auf wei- tere geschützte interne IT-Systembereiche der Beschwerdeführerin in mehreren Fällen erfolgreich gewesen. Im Forensikbericht seien unter Angabe von genauen Start- und Endzeiten die einzelnen "Eingriffe" auf Kundendaten unbeteiligter (nicht einwilligender) Kunden doku- mentiert. Bei sämtlichen Bewegungen habe es dem Beschuldigten klar sein müssen, dass er sich im System der Beschwerdeführerin auch nicht lateral bewegen dürfe. Die mehrstufigen Sicherheitsmassnahmen zeigten, dass der Zugriff auf die internen Systeme nicht offen ge- wesen sei, sondern durch verschiedene technische und organisatorische Vorkehrungen um- fassend geschützt worden sei. Die Aussage des Zeugen, dass lateral keine Sicherheitsvor- kehrungen bestanden hätten, sei nicht zutreffend. Dessen Aussage sei unter der Prämisse der langen Dauer der Befragung zu sehen.

E. 3.7

Die Staatsanwaltschaft argumentiere, dass für einen Datenabfluss vom System der Beschwerdeführerin hin zum Beschuldigten Spuren in technischer Hinsicht fehlen würden und

Seite 13/20 berufe sich dabei auf den Zeugen V._____. Auch diesbezüglich werde auf die Befra- gungsdauer von über acht Stunden hingewiesen, was die Qualität der Aussage des Zeugen beeinträchtigt haben könnte. Im Forensikbericht würden die Tools des Angreifers als Be- weismittel aufgeführt und dem Beschuldigten zugeordnet. Auf dem PC des Beschuldigten seien die Dateien AQ._____, AR._____, AS._____ und AT._____ gefunden worden. Dabei sei offensichtlich, dass ein solcher Datenbaum in den Daten der Beschwerde- führerin nicht zu erwarten sei. AJ._____ sei das Programm des Beschuldigten. Diese Tools seien sowohl in den entsiegelten Daten als auch im System der Beschwerdeführerin gefunden worden. Die Tools (AQ._____ und AS._____) befänden sich widerrechtlich im IT-System der Beschwerdeführerin. Somit seien sowohl in den beschlagnahmten und ent- siegelten Daten wie auch im Forensikbericht die identischen Spuren der Tools des Beschul- digten vorgefunden worden. Der Beschuldigte habe die Logindaten von Kunden für den uner- laubten Zugang in das System der Beschwerdeführerin verwendet. Er habe die Tools gezielt eingesetzt, um auf sensible Daten

zuzugreifen und diese möglicherweise zu manipulieren oder weiterzugeben. Ob der Beschuldigte die Daten abfotografiert oder auf andere Weise kopiert habe, sei nicht von Bedeutung. Fakt sei, dass er unbefugt auf die internen Systeme zugegriffen und die Daten eingesehen und genutzt habe.

E. 3.8

Entgegen der Auffassung der Staatsanwaltschaft sei es grundsätzlich möglich, dass gleichzeitig überschneidende Remote-Desktop-Sitzungen stattfänden, somit mehrere Benutzer gleichzeitig auf ein System zugreifen könnten, wenn der Remote-Desktop-Dienst diese Funk- tion unterstütze. Die gegenteilige Annahme des Zeugen sei wiederum wohl auf dessen Er- müdung wegen der langen Dauer der Befragung zurückzuführen. Der Beschuldigte habe sich über mehrere Server hinweg weiterverbunden und sich mit verschiedenen Benutzerdaten über RDP (Remote Desktop Protocol) eingeloggt. Während er eingeloggt gewesen sei, habe er zusätzlich versucht, über Windows-Freigaben auf weitere Ressourcen zuzugreifen, um Daten zu kopieren oder zu manipulieren.

E. 3.9

Die Staatsanwaltschaft habe lediglich die entsiegelten Daten aus der Hausdurchsuchung ausgewertet, jedoch nicht forensisch. Darüber hinaus habe sie weder die Evidenzen des Forensikberichts geprüft noch einen ganzheitlichen Einblick in die Systemarchitektur der Beschwerdeführerin vorgenommen. Es sei daher erforderlich, dass die Zuger Polizei die Unter- suchungen mit Bezug auf die Fragestellungen der Staatsanwaltschaft mittels ganzheitlichem Einblick in die Systemarchitektur der Beschwerdeführerin durchführe.

E. 3.10

Die Staatsanwaltschaft habe dem Beschuldigten zu Unrecht eine Entschädigung und Genug- tuung sowie eine Entschädigung für seine Wahlverteidigung ausgerichtet. Die Staatsanwalt- schaft verkenne dabei, dass der Beschuldigte die Ursache für die Strafanzeige in zivilrecht- lich vorwerfbarer Weise gesetzt habe.

E. 4

Die Staatsanwaltschaft wurde von der Beschwerdeabteilung des Obergerichts im Beschluss vom 28. September 2022 wie erwähnt angewiesen, abzuklären, ob (i) der Beschuldigte weitergehende Informationen oder Daten aus den Systemen der Beschwerdeführerin beschafft habe, als dies über das Kundenlogin möglich gewesen sei, ob (ii) der Beschuldigte in die interne IT-Systeminfrastruktur der Beschwerdeführerin eingedrungen sei, ob (iii) er dadurch Kundendaten oder andere Informationen erlangt und ob (iv) er Programme in die Systemum- gebung der Beschwerdeführerin implementiert habe. Sodann hielt die Beschwerdeabteilung

Seite 14/20 fest, dass die Staatsanwaltschaft zu klären habe, ob die in diesem Zusammenhang gemach- ten Feststellungen im Forensikbericht vom 30. Oktober 2020 und die daraus gezogenen Schlüsse der Beschwerdeführerin zutreffend seien.

E. 4.1

Die Staatsanwaltschaft hat in diesem Zusammenhang der Zuger Polizei am 28. November 2022 einen Ermittlungsauftrag erteilt, welcher mit Rapport vom 28. August 2024 abgeschlos- sen wurde. Des Weiteren hat die Staatsanwaltschaft am 24. November 2022 bei der K._____ AG Unterlagen im Zusammenhang mit der Erstellung des AD._____

Report vom 30. Oktober 2020 eingefordert, wobei die K._____ AG dieser Aufforderung mit Schreiben vom 2. Dezember 2022 nachgekommen ist. Sodann befragte die Staatsanwalt- schaft am 26. Juni 2023 den Ersteller des AD._____ Report, V._____, als Zeugen und führte am 8. März 2024 eine Einvernahme mit dem Beschuldigten durch. Schliesslich hiess das Zwangsmassnahmengericht den Antrag der Staatsanwaltschaft betreffend Entsie- gelung der am 7. April 2021 versiegelten Aufzeichnungen und Gegenstände der H._____ GmbH und des Beschuldigten mit Verfügung vom 29. Dezember 2023 teilweise gut.

E. 4.2

Es stellt sich die Frage, ob diese von der Staatsanwaltschaft ergänzend durchgeführten Untersuchungshandlungen ausreichend waren, um die von der Beschwerdeführerin in ihrer Strafanzeige vorgebrachten Vorwürfe gegen den Beschuldigten und/oder allenfalls unbekannte Täterschaft rechtsgenügend abzuklären, und ob sie darüber hinaus aufgrund des Untersuchungsergebnisses die Strafuntersuchung einstellen durfte.

E. 5

Die Staatsanwaltschaft verfügt die vollständige oder teilweise Einstellung des Verfahrens, wenn kein Straftatbestand erfüllt oder kein Tatverdacht erhärtet ist, der eine Anklage rechtfertigt (Art. 319 Abs. 1 lit. a und b StPO).

E. 5.1

Der Entscheid über die Einstellung des Verfahrens richtet sich nach dem aus dem Legalitätsprinzip fliessenden Grundsatz "in dubio pro duriore" (vgl. Art. 5 Abs. 1 BV und Art. 2 Abs. 1 StPO i.V.m. Art. 319 Abs. 1 und Art. 324 Abs. 1 StPO). Demzufolge darf eine Einstel- lung durch die Staatsanwaltschaft nur bei klarer Straflosigkeit, namentlich fehlendem Tatver- dacht bzw. offensichtlich fehlenden Prozessvoraussetzungen verfügt werden. Ist eine Verur- teilung wahrscheinlicher als ein Freispruch, ist, sofern die Erledigung mit einem Strafbefehl nicht in Frage kommt, Anklage zu erheben. Dasselbe gilt in der Regel, wenn ein Freispruch ebenso wahrscheinlich wie eine Verurteilung erscheint. Der Grundsatz, dass im Zweifelsfall nicht eingestellt werden darf, ist unter Würdigung der im Einzelfall gegebenen Umstände an- zuwenden. Bei zweifelhafter Beweis- bzw. Rechtslage hat mithin nicht die Untersuchungs- oder Anklagebehörde über die Stichhaltigkeit des strafrechtlichen Vorwurfs zu entscheiden, sondern das für die materielle Beurteilung zuständige Gericht. Jedoch sind Sachverhaltsfest- stellungen unter Berücksichtigung des Grundsatzes "in dubio pro duriore" auch bei Einstel- lungen zulässig, soweit gewisse Tatsachen "klar" bzw. "zweifelsfrei" feststehen, so dass im Fall einer Anklage mit grosser Wahrscheinlichkeit keine abweichende Würdigung zu erwarten ist. Der Staatsanwaltschaft ist es mithin nur bei unklarer Beweislage untersagt, der gerichtlichen Beweiswürdigung vorzugreifen. Den kantonalen Instanzen steht bei der Überprüfung von Einstellungsverfügungen ein gewisser Ermessensspielraum zu (BGE 143 IV 241 E. 2.2.1; 138 IV 186 E 4.1; Urteil des Bundesgerichts 6B_1195/2019 vom 28. April 2020 E. 3.1; je m.H.).

E. 5.2

Die Klärung des Sachverhalts ist dabei Aufgabe der Staatsanwaltschaft. Die Strafbehörden haben von Amtes wegen alle für die Beurteilung der Tat und der beschuldigten Person be-

deutsamen Tatsachen abzuklären (Art. 6 Abs. 1 StPO). Sie untersuchen die belastenden und entlastenden Umstände mit gleicher Sorgfalt (Art. 6 Abs. 2 StPO). Sie setzen zur Wahrheits- findung alle nach dem Stand von Wissenschaft und Erfahrung geeigneter Beweismittel ein, die rechtlich zulässig sind (Art. 139 Abs. 1 StPO). Zur Ermittlung der Wahrheit haben sie von den bestmöglichen Beweismitteln Gebrauch zu machen (Wohlers, in: Donatsch und andere [Hrsg.], Kommentar zur Schweizerischen Strafprozessordnung, 3. A. 2020, Art. 6 StPO N 9).

E. 5.3

Die Beschwerdeführer bezichtigen den Beschuldigten und/oder eine unbekannte Täterschaft der unbefugten Datenbeschaffung, des unbefugten Eindringens in ein Datenverarbeitungs- system und des unbefugten Beschaffens von Personendaten.

E. 5.3.1

Gemäss Art. 143 StGB macht sich strafbar, wer in der Absicht, sich oder einen andern unrechtmässig zu bereichern, sich oder einem andern elektronisch oder in vergleichbarer Weise gespeicherte oder übermittelte Daten beschafft, die nicht für ihn bestimmt und gegen seinen unbefugten Zugriff besonders gesichert sind.

E. 5.3.2

Nach Art. 143bis StGB wird auf Antrag bestraft, wer auf dem Wege der Datenübertragungs- einrichtungen unbefugterweise in ein fremdes, gegen seinen Zugriff besonders gesichertes Datenverarbeitungssystem eindringt.

E. 5.3.3

Gemäss Art. 179novies StGB wird auf Antrag bestraft, wer unbefugt besonders schützenswerte Personendaten oder Persönlichkeitsprofile, die nicht frei zugänglich sind, aus einer Daten- sammlung beschafft.

E. 6

Die Beschwerdeführerin wirft der Staatsanwaltschaft zunächst vor, den AD._____ Report nicht analysiert und somit die massgebenden von der Beschwerdeführerin in der Strafanzei- ge beigebrachten Beweismittel nicht geprüft zu haben. Die Staatsanwaltschaft wolle das Ver- fahren lediglich aufgrund der von ihr bzw. der Zuger Polizei ausgewerteten Daten einstellen, was nicht zulässig sei.

E. 6.1

Dazu ist zunächst festzuhalten, dass die Staatsanwaltschaft entsprechend der Weisung der Beschwerdeabteilung des Obergerichts abgeklärt hat, ob die im Bericht der K._____ AG gemachten Feststellungen und die gestützt auf diesen Bericht von der Beschwerdeführerin gegenüber dem Beschuldigten erhobenen Vorwürfe zutreffend sind. Die Ergebnisse dieser Abklärungen fanden Eingang in den Rapport der Zuger Polizei vom 28. August 2024 (HD 10/43 ff.). Insbesondere wurde festgehalten, dass verschiedene Feststellungen im Be- richt der K._____ AG, einem von der Beschwerdeführerin in Auftrag gegebenen Privat- gutachten, unzutreffend sind und dieser Bericht im Übrigen Mängel aufweist, wie sich bei der Befragung des Zeugen V._____ herausstellte. Dieser gab – als Ersteller des AD._____ Report – gemäss Polizeirapport denn auch selber an, dass dieser Bericht ver- schiedene Fehler aufweise (Vi act. 22/5/1 ff.). Sodann äusserte V._____ noch die Vermu- tung, er gehe davon aus, dass Endkunden der

Beschwerdeführerin dem Beschuldigten Zu- griff auf die Systeme der Beschwerdeführerin gegeben hätten. Damit werden Aussagen des Beschuldigten wie auch der befragten ehemaligen Kunden der Beschwerdeführerin gestützt,

Seite 16/20 welche angaben, dass sie dem Beschuldigten Zugriff auf ihre Daten und Systeme gegeben haben (Vi act. 22/1-4).

E. 6.2

Dass das Obergericht den Bericht im Beschluss vom 28. September 2022 als Forensikbericht bezeichnet hat, wie die Beschwerdeführerin betont (vgl. act. 1 Rz 9), ändert daran nichts. Das Obergericht hielt damals denn auch einschränkend fest, dass die Staatsanwaltschaft nicht erklärt habe, weshalb der Forensikbericht und die daraus abgeleiteten Schlussfolgerun- gen der Beschwerdeführerin unzutreffend sein sollten (vgl. vorne Sachverhalt Ziff. 6.3). Dies holte die Staatsanwaltschaft nun nach. Sodann ist nicht zu beanstanden, dass keine weiteren Mittel eingesetzt wurden, um die Rohdaten der K._____ AG lesbar zu machen, um die Evidenzen zu analysieren. Mit der Staatsanwaltschaft ist davon auszugehen, dass die (ins- besondere belastenden) Daten Eingang in den Bericht gefunden haben und die Rohdaten mithin keine weiteren Erkenntnisse zu liefern vermöchten. Schliesslich basiert der Einwand der Beschwerdeführerin, wonach AK._____ vom Dienst Cyber- und Wirtschaftsdelikte der Zuger Polizei die notwendige Qualifikation zur Analyse des Berichts gefehlt habe, lediglich auf einer Mutmassung, welche mit einem Hinweis auf sein Linkedin Profil nicht belegt werden kann (vgl. act. 1 Rz 30).

E. 6.3

Weiter gab der Ersteller des Berichts, V._____, als Zeuge zwar zu Protokoll, dass ihm von der Beschwerdeführerin eine IP-Adresse (R._____) mitgeteilt worden sei, welche als ungewöhnlich aufgefallen sei (Vi act. 10/47 Frage 26). Im Polizeirapport wird jedoch ausge- führt, dass mit den von K._____ AG zur Verfügung gestellten Daten, welche beschlag- nahmt worden seien, die in der Strafanzeige formulierten Vorwürfe nicht bewiesen und/oder erhärtet werden könnten (Vi act. 10/50 f.). Ein Zugriff, wie in der Strafanzeige behauptet, konnte von der Zuger Polizei nicht festgestellt werden. Diese weist denn auch darauf hin, dass bei den am 24. November 2022 bei der K._____ AG edierten Unterlagen eine Audio-Datei enthalten sei, welche gemäss dem Ersteller des AD._____ Report beim ers- ten Zusammentreffen mit der Beschwerdeführerin erstellt worden sei. Der Inhalt dieser Audio-Datei erwecke den Eindruck, dass die Beschwerdeführerin schon vor den Abklärungen durch die K._____ AG den Beschuldigten für die in der Strafanzeige aufgeführten Taten verantwortlich mache (Vi act. 10/50). Dies erweckt grundsätzlich Zweifel an der Objektivität des Berichts, zumal V._____ kein ganzheitlicher Einblick in die Daten der Beschwerde- führerin gewährt wurde (vgl. hinten E. 6.4). Die Staatsanwaltschaft weist in diesem Zusam- menhang auch darauf hin, dass basierend auf der Strafanzeige und dem AD._____ Re- port anlässlich der diversen Triage-Verhandlungen unter der Leitung des Zwangsmassnah- mengerichts die sichergestellten Systeme des Beschuldigten bzw. der H._____ GmbH mit Stichworten durchsucht worden seien. So sei [da in den protokollierten Sessions der Be- schwerdeführerin gemäss den Erkenntnissen der K._____ AG die Workstation "AL._____" identifiziert werden konnte und die Beschwerdeführerin darin eine Verbin- dung zur H._____ GmbH vermutet, welche ihr Domizil an der AL._____ in

AM._____ hatte] nach "AL._____" allein oder nach "AL._____" and/not "AL._____" gesucht worden, sowie nach AO._____ oder AN._____. Ausserdem seien diverse Server-Namen und weitere Stichworte eingegeben worden. Mit den vom Zwangsmanssnahmengericht letztlich freigegebenen Daten und Unterlagen hätten die in der Strafanzeige formulierten Vorwürfe jedoch nicht bewiesen bzw. erhärtet werden können. Auch der Zeuge V._____ führte an der Einvernahme aus, dass man einen Host mit dem

Seite 17/20 Namen "AL._____" auf den Systemen des Angreifers hätte finden müssen (Vi act. 22/5/19; zu den Suchbegriffen AO._____ und AN._____ vgl. hinten E. 6.8).

E. 6.4

Ferner wies V._____ im Rahmen seiner Zeugenbefragung (Vi act. 22/5/1 ff.), wie erwähnt, selber auf Unstimmigkeiten und Fehler im Bericht hin. Offenbar konnten auch keine Firewall-Logdaten analysiert werden, da solche gemäss Mitteilung der Beschwerdeführerin nicht vorhanden seien. V._____ gab zu Protokoll, dass er bei der Beschwerdeführerin die Firewall-Logdaten lediglich angefordert habe. Von dieser habe er die Rückmeldung erhalten, dass solche Logdaten nicht vorhanden seien. Dies habe er nicht selber verifiziert (Vi act. 22/5/13). Der Bericht weist sodann auch insoweit Mängel auf, als nicht erklärbar ist, wie die externe IP-Adresse R._____ auf die Kundenserver geloggt sein konnte, wenn der Zugriff jeweils über die Kundengeräte bzw. über O._____ erfolgt ist. Die Beschwerdeführerin führt zwar aus (act. 1 Rz 71), dass gemäss Bericht der K._____ AG die meisten Zugriffe über die Kundengeräte erfolgt seien, doch nicht alle. Die übrigen Zugriffe seien über die Firewall erfolgt. Diese Behauptung ist indes schon deshalb nicht nachvollziehbar, da V._____ die Firewall-Logdaten von der Beschwerdeführerin mit der Begründung nicht zugänglich gemacht wurden, dass solche Logdaten nicht vorhanden seien (Vi act. 22/5/13). Befinden sich aber im Bericht der K._____ AG keine Informationen zur Firewall, so be- stehen jedenfalls keine belegbaren Hinweise dafür, dass ein allfälliger Zugriff betreffend die IP-Adresse R._____ über die Firewall der Beschwerdeführerin hätte erfolgen können. Un- ter diesen Umständen ist die Möglichkeit einer Manipulation der Logdaten, wie sie der Be- schuldigte vermutet (act. 6 Rz 84), jedenfalls nicht von der Hand zu weisen. Aufgrund der erwähnten Unstimmigkeiten im Bericht der K._____ AG ist jedenfalls nicht zu beanstan- den, dass die Staatsanwaltschaft nicht unbesehen darauf abgestellt, sondern die im Raum stehenden Vorwürfe durch weitere Ermittlungen (insbesondere Auswertung der durch das Zwangsmassnahmengericht freigegebenen Daten und Unterlagen) abgeklärt hat. Diese bestätigten denn die Erkenntnisse aus dem Bericht der K._____ AG nicht (vgl. vorne E. 6.3). Bei dieser Sachlage ist vor allem auch aus Gründen der Verhältnismässigkeit nicht zu beanstanden, dass die Staatsanwaltschaft auf weitere Abklärungen zum Bericht der K._____ AG, insbesondere auf eine forensische Auswertung, verzichtete.

E. 6.5

Die Beschwerdeführerin vermag auch mit ihren Ausführungen zu den Lateralen Bewegungen (Beschwerde Rz 74 ff.) – d.h. der Ausbreitung im System nach einem initialen Zugriff – kei- nen hinreichenden Verdacht auf ein strafrechtlich relevantes Verhalten des Beschuldigten aufzuzeigen. Soweit sie geltend macht, die Täterschaft habe bei ihren Handlungen Sicher- heitsschranken überwinden müssen, widerspricht sie dem Zeugen V._____, welcher als Ersteller des Berichts der K._____ AG sinngemäss ausführte, dass bei der Beschwerde- führerin keine internen Sicherheitsschranken bestanden hätten (Vi

act. 22/5/14). Auch die von der Beschwerdeführerin erwähnte WhatsApp-Kommunikation vermag ein strafrechtlich relevantes Verhalten des Beschuldigten nicht als wahrscheinlich erscheinen zu lassen. Diese Kommunikation könnte ihren Grund ohne Weiteres auch darin gehabt haben, dass die Be- schwerdeführerin ihre Daten – wie von den befragten Zeugen als ehemalige Kunden der Be- schwerdeführerin bestätigt – teilweise verschlüsselt habe und eine Entschlüsselung im Rah- men einer Weitergabe an die H._____ GmbH erfolgt ist.

E. 6.6

Was den behaupteten Datenabfluss (Beschwerde Rz. 89 ff.) aus dem System der Beschwer- deführerin betrifft, so ist auf die Aussage des Zeugen V._____ hinzuweisen, wonach kei-

Seite 18/20 ne Firewall-Logs verfügbar seien, welche einen Datenabfluss belegen würden (Vi act. 22/5/6). Weiter weist die Beschwerdeführerin zwar darauf hin, dass fehlende Einträge auf der Firewall nicht zwingend bedeuten, dass kein Datenfluss stattgefunden habe, könnten die geöffneten Dateien doch auch abfotografiert oder auf andere Weise kopiert worden sein (act. 1 Rz 104 f.). Dies hat die Staatsanwaltschaft nicht übersehen. Mangels Spuren in techni- scher Hinsicht fehlen indes verwertbare Hinweise auf einen Datenabfluss und mithin auf ein tatbestandsmässiges Verhalten. In den durch das Zwangsmassnahmengericht freigegebe- nen Daten und Unterlagen konnten denn offenbar auch keine Hinweise auf abgeflossene Kundendaten gefunden werden.

E. 6.7

Auch wenn die Beschwerdeführerin wiederholt mit Ermüdungserscheinungen des Zeugen aufgrund der langen Befragungsdauer argumentiert – so auch hinsichtlich der Antwort bezüg- lich der Möglichkeit gleichzeitig überschneidender Remote-Desktop-Sitzungen (Beschwerde Rz 107 ff.; Vi act. 22/5/16) –, ist festzuhalten, dass sich der Zeuge als Ersteller des Berichts der K._____ AG mit Sicherheit auf die Befragung vorbereitet hatte und die Fragen wahr- heitsgetreu zu beantworten in der Lage war. Der Zeuge wurde denn auch auf die Wahrheits- pflicht aufmerksam gemacht und die damalige Rechtsvertreterin der Beschwerdeführerin hät- te anlässlich der Zeugenbefragung zu dieser Thematik Ergänzungsfragen stellen können. Im Übrigen wurde die Befragung nicht am Stück durchgeführt, sondern sie wurde für Pausen un- terbrochen. Zudem war die Privatklägerin, wie bereits erwähnt, an der Einvernahme anwalt- lich vertreten und hätte im Falle einer möglicherweise zu langen Dauer der Befragung inter- venieren können (Vi act. 22/5/1).

E. 6.8

Soweit die Beschwerdeführerin in der Beschwerde Rz. 91 ff. die Tools aufführt, mit welchen der Beschuldigte in ihr System eingedrungen sein soll, so kann wiederum auf die Aussagen des Zeugen V._____ verwiesen werden, welcher ausführte, dass sich die entsprechen- den Tools (AQ._____, AR._____, AS._____ und AT._____) nicht von norma- ler Software unterscheiden würden und auch nicht für einen Angriff taugten. Insbesondere könnten damit nicht irgendwelche Sicherheitsschranken umgangen werden. Man benutze die Tools zur Ausleitung von Daten, nicht zum Eindringen (Vi act. 22/5/19). In diesem Zusam- menhang weist der Beschuldigte zutreffend darauf hin, dass er seinen Kunden erwiesener- massen bei der Migration ihrer Daten geholfen habe (act. 6 Rz 88). Auch diesbezüglich er- geben sich somit keine konkreten Anhaltspunkte für ein tatbestandsrelevantes Verhalten des Beschuldigten hinsichtlich der ihm gegenüber erhobenen Vorwürfe, insbesondere des Ein- dringens in ein gegen seinen Zugriff besonders

gesichertes Datenverarbeitungssystem, wie für eine Tatbestandserfüllung nach Art. 143 StGB vorausgesetzt. Die Beschwerde erweist sich insoweit als unbegründet.

E. 6.9

Bei dieser Sachlage ist nicht mehr auf den Einwand der Beschwerdeführerin einzugehen, wonach die Staatsanwaltschaft die Verwertbarkeit der durch die Software AC._____ gewonnenen Daten zu Unrecht in Frage gestellt hat (act. 1 Rz 35 ff.). Es ist in diesem Zusammenhang lediglich darauf hinzuweisen, dass sich auch die Staatsanwaltschaft an rechtlich zulässige Beweismittel zu halten hat (vgl. Art. 139 Abs. 1 StPO).

E. 7

Nicht einzutreten ist auf die Beschwerde schliesslich insoweit, als die Beschwerdeführerin beantragt, die Verfahrenskosten im Untersuchungsverfahren seien dem Beschuldigten aufzuerlegen, dem Beschuldigten sei keine Entschädigung und Genugtuung für sich und keine

Seite 19/20 Entschädigung für seine Wahlverteidigung auszurichten (Anträge Ziff. 2.3-2.5). Die Staats- anwaltschaft hat die Verfahrenskosten auf die Staatskasse genommen und dem Beschuldig- ten eine Entschädigung für seine Wahlverteidigung sowie für ihn persönlich eine Entschädi- gung und Genugtuung aus der Staatskasse ausgerichtet (Dispositiv-Ziff. 2-4). Die Beschwer- deführerin ist folglich von diesen Dispositivziffern nicht beschwert. Sie hat daher kein im Sin- ne von Art. 382 Abs. 1 StPO rechtlich geschütztes Interesse an deren Aufhebung, weshalb ihr diesbezüglich Beschwerdelegitimation fehlt.

E. 8

Die Staatsanwaltschaft hat nach dem Gesagten zu Recht erwogen, dass sich auch nach Durchführung der ergänzenden Beweisabnahmen keine konkreten Anhaltspunkte dafür ergeben, welche die Anschuldigungen gemäss Strafanzeige und die Erkenntnisse des Berichts der K._____ AG bestätigen würden. Bei dieser Sachlage ist nicht zu beanstanden, dass die Staatsanwaltschaft im Rahmen des ihr zustehenden Ermessensspielraums die Strafuntersuchung gegen den Beschuldigten betreffend unbefugte Datenbeschaffung, unbefugtes Eindringen in ein Datenverarbeitungssystem und unbefugtes Beschaffen eingestellt hat, kann doch nicht mehr gesagt werden, dass eine Verurteilung ebenso wahrscheinlich ist wie ein Freispruch. Die Beschwerde erweist sich als unbegründet und ist abzuweisen, soweit darauf einzutreten ist. Damit sind auch die Anträge Ziff. 3.1.-3.11. der Beschwerdeführerin abzuwei- sen. Die Beschwerdeabteilung kann der Staatsanwaltschaft einzig bei der Gutheissung der Beschwerde gegen eine Einstellungsverfügung für den weiteren Gang des Verfahrens Wei- sungen erteilen (Art. 397 Abs. 3 StPO).

E. 9

Bei diesem Ausgang sind die Kosten des Beschwerdeverfahrens der Beschwerdeführerin aufzuerlegen (Art. 428 Abs. 1 StPO). Der Beschuldigte, der eine Stellungnahme einreichen und die Abweisung der Beschwerde beantragen liess, ist mit seinem Standpunkt im vorliegenden Verfahren durchgedrungen. Gemäss bundesgerichtlicher Rechtsprechung (BGE 147 IV 47 E. 4.2.5) wird die unterliegende Privatklägerschaft, soweit sie den Rechtsweg allein beschreitet, der beschul- digten Person sowohl im Berufungs- wie im Beschwerdeverfahren entschädigungspflichtig, wenn es um ein Antragsdelikt geht (Art. 436 Abs. 1 in Verbindung mit Art. 432 Abs. 2 StPO). Bei von Amtes wegen zu verfolgenden Delikten trägt hingegen die gegen eine Einstellungs- verfügung Beschwerde führende Privatklägerschaft ein latent weiterbestehendes öffentliches Strafverfolgungsinteresse mit,

da der staatliche Strafverfolgungsanspruch erst mit einem frei- sprechenden Urteil abschliessend eingelöst wird. Im Beschwerdeverfahren betreffend Offizi- aldelikte hat daher – im Gegensatz zum Berufungsverfahren – der Staat und nicht die unter- liegende Privatklägerschaft die beschuldigte Person zu entschädigen. Das vorliegende Verfahren betrifft im Hauptpunkt ein Offizialdelikt (Unbefugte Datenbeschaf- fung, Art. 143 StGB). Der Beschuldigte ist mithin vom Staat für seinen notwendigen Aufwand im Beschwerdeverfahren (Art. 429 Abs. 1 in Verbindung mit Art. 436 Abs. 1 StPO) angemes- sen zu entschädigen. Zur Parteienschädigung ist mangels eines Antrags keine Mehrwert- steuer hinzuzurechnen (vgl. Weisung des Obergerichts über die Mehrwertsteuer in der Zivil- und Strafrechtspflege des Kantons Zug vom 29. Juli 2015).