Rechtlicher und technischer Hintergrund des „EMS-Skandals“

Welcher Straftatbestand wurde uns konkret vorgeworfen?

Der Vorwurf gegen epicenter.works lautete auf § 118a StGB „Widerrechtlicher Zugriff auf ein Computersystem“ und darüber hinaus auf die Qualifikation des § 118a Abs. 2 StGB in Bezug auf ein Computersystem, das ein wesentlicher Bestandteil der kritischen Infrastruktur (§ 74 Abs. 1 Z 11) ist. Damit waren wir mit einer Strafdrohung von bis zu zwei Jahren Freiheitsstrafe konfrontiert.

Zu beachten ist, dass es sich bei § 118a StGB um ein sogenanntes Ermächtigungsdelikt handelt, sodass eine Strafverfolgung nur dann erfolgen kann, wenn eine Ermächtigung des Geschädigten vorliegt. Diese Ermächtigung wurde im vorliegenden Fall durch den zuständigen Gesundheitsminister Wolfgang Mückstein erteilt und von seinem Nachfolger Gesundheitsminister Johannes Rauch auf unsere Bitte hin auch nicht zurückgenommen.

Warum wurde die Strafverfolgung eingestellt?

Eine Strafbarkeit nach § 118a StGB liegt nur dann vor, wenn auch die entsprechenden subjektiven Tatbestandsmerkmale erfüllt sind. Diese sind dann gegeben, wenn:

1. Spionageabsicht: der Zugriff auf ein Computersystem in der Absicht erfolgt, sich oder einem anderen Unbefugten Kenntnis von personenbezogenen Daten zu verschaffen. Kenntnis der Daten muss schutzwürdige Geheimhaltungsinteressen der Betroffenen verletzen.
2. Schädigungsabsicht: durch die Verwendung des Computersystems oder der daraus erlangten Daten einer Person ein Nachteil zugefügt wird.

Beides lag im vorliegenden Fall nicht vor. Als Datenschutzverein haben wir natürlich im Vorhinein das Einverständnis aller Personen eingeholt, deren Daten zur Verifikation der Echtheit des EMS abgefragt wurden. Eine Schädigungsabsicht kann deshalb nicht vorgelegen haben, da wir lediglich die Echtheit einer Lücke, die uns gemeldet wurde, verifizierten, um sie umgehend durch die Verantwortlichen schließen zu lassen. Unser Handeln hat Schaden von Betroffenen abgewendet.

Auch die objektiven Tatbestandsmerkmale lagen nicht vor, da wir ja lediglich eine bestehende Sicherheitslücke als zugezogene Expert:innen eines Mediums bewerteten und dokumentierten.

Was unterscheidet ethischen Umgang mit Sicherheitslücken von Computerkriminalität?

Sicherheitsforschung, die auch oft im universitären Bereich stattfindet oder bei staatlichen Cybersicherheits-Challenges, und Computerkriminelle verwenden grundsätzlich dieselben Methoden und Werkzeuge. Die Sicherheit eines Systems zu prüfen ist sehr oft nur möglich, indem es auf Schwachstellen getestet wird. Ob eine Schwachstelle wirklich besteht, kann nur durch ihre Anwendung geprüft werden. Wenn ein Schlosser versucht die Sicherheit eines Schlosses zu bewerten, versucht er es auch ohne Schlüssel zu öffnen.

Der große Unterschied zwischen Kriminellen und richtig handelnden Sicherheitsforscher:innen liegt darin, wie mit dieser Sicherheitslücke umgegangen wird. Es gibt seit Jahrzehnten das Konzept der „*Responsible Disclosure*“[1] für den richtigen Umgang mit Sicherheitslücken. Dabei meldet die:der Sicherheitsforscher:in die Schwachstelle an den Hersteller oder Verantwortlichen, damit diese Lücke geschlossen wird. Erst nachdem die Gefahr gebannt ist, wird öffentlich über die Schwachstelle berichtet. In vielen Ländern gibt es genau dafür rechtliche Absicherungen. Das ist, was die Wissenschaft fordert und auch die EU-Behörde für IT-Sicherheit „ENISA“ spricht sich dafür aus.

Wenn eine Sicherheitslücke nicht gemeldet und geschlossen wird, kann sie auch für Angriffszwecke ausgenutzt werden, um Schaden anzurichten oder Daten abzugreifen. Durch eine Meldung hingegen wird dieser Schaden ausgeschlossen und die Sicherheit für alle verbessert. Trotzdem ist die Meldung von Sicherheitslücken an Hersteller oder Verantwortliche oft die Option, von der Sicherheitsforscher:innen sich nicht nur keinen Vorteil erwarten dürfen, sondern sogar oft mit strafrechtlichen Konsequenzen bedroht werden. (wie in unserem Fall)

Wieso hat das alles so lange gedauert?

Uns ist absolut unverständlich, wieso wir **ein Jahr lang nicht über die Anzeige und das Ermittlungsverfahren gegen uns informiert** wurden. Hier hätte eine umgehende Information ergehen müssen. Scheinbar war die technische Komplexität des Verfahrens ein Grund, wieso die ermittelnden Stellen nur sehr langsam zur Bearbeitung des Falles schritten. Die erste Kommunikation der ermittelnden Behörden an uns war auch begleitet von der Bitte, den (technischen) Sachverhalt zu erklären.

Sobald wir dem zuständigen Staatsanwalt in Innsbruck den Sachverhalt darlegen konnten, hat er entschieden, das Verfahren gegen uns einzustellen. Jedoch war das Verfahren gegen uns mit dem Verfahren der HG Lab Truck[2] zusammengezogen, da deren sorgloser Umgang diese Sicherheitslücke erst möglich gemacht hat. Dadurch war der gesamte Akt als „clamoroses Verfahren“ eingestuft und berichtspflichtig.

Bei einem berichtspflichtiges Verfahren muss der:die zuständige Staatsanwält:in jede Entscheidung zuerst durch die Weisungskette absegnen lassen. Das bedeutet: die Oberstaatsanwaltschaft und letztendlich das Justizministerium müssen zustimmen. Somit mussten wir annähernd **ein weiteres Jahr** warten bis das Verfahren gegen uns endgültig eingestellt wurde, was uns noch weitere Anwaltskosten und Nerven kostete. Über die Einstellung des Verfahrens wurde unsere Anwältin Maria Windhager telefonisch verständigt. Auf eine Einstellungsbegründung warten wir immer noch.

Das war kein Einzelfall: Warum bedarf es einer gesetzlichen Änderung?

Auch wenn letztlich keine Anklage erhoben wurde, waren die **Kosten von rund 15.000 EUR** und der Zeitaufwand für epicenter.works enorm. Wir sind der Meinung, dass dieser Aufwand unabhängige Sicherheitsforscher:innen, NGOs oder Journalist:innen in Zukunft davon abhalten könnte, mögliche Sicherheitslücken überhaupt zu untersuchen oder, nachdem diese geschlossen wurden, über sie zu berichten. Genau das Verhalten, das der gesamtgesellschaftlichen Sicherheit und einer demokratischen Debatte über realistische Bedrohungsszenarien dienen würde, wird durch die

1 https://de.wikipedia.org/wiki/Responsible_Disclosure_(IT-Sicherheit) Synonym: „coordinated disclosure“
2 https://www.derstandard.at/story/2000133001435/erste-klagen-wegen-datenleck-bei-hg-lab-truck-eingebracht

aktuelle gesetzliche Lage also u.U. bestraft, bzw. durch das hohe rechtliche Risiko und den enormen Aufwand zumindest sehr unattraktiv. Und das zu einem Zeitpunkt, an dem immer mehr Staaten und internationale Organisationen zu verstehen beginnen, welchen Mehrwert Sicherheitsforschung für die Allgemeinheit und die Cybersicherheit im Besonderen generieren kann.[3]

Zu beachten ist weiters, dass der Tatbestand des § 118a StGB zwar äußerst selten zur Anwendung gelangt, zumal die Beweisführung äußerst schwierig ist. Dadurch geraten aber gerade Sicherheitsforscher:innen, die die Information über die Sicherheitslücke bewusst an die Verantwortlichen weitergeben und damit den Schutz vor Angriffen verbessern würden, besonders leicht ins Visier von Ermittlungen. Das führt zur paradoxen Situation, dass aus Sicht der Sicherheitsforscher:innen ein ethisches Verhalten „bestraft" wird und somit das übergeordnete rechtspolitische Ziel, welches mit dem § 118a StGB verfolgt wird, gerade eben nicht erreicht wird: nämlich der Schutz vor IT-Attacken (dem „Widerrechtlichen Zugriff auf ein Computersystem").

Was sagt die Wissenschaft und das Justizministerium dazu?

Dass Sicherheitsforschung, die sich an *Responsible-Disclosure*-Regeln hält, eigentlich nicht unter den Straftatbestand des § 118a StGB fallen sollte, wird von der Wissenschaft schon länger vertreten[4][5]. Seit August 2023 gibt es dazu auch einen entsprechenden Erlass[6] des Justizministeriums. Diese Rechtsmeinung an sich schützt aber noch nicht die korrekt handelnden Sicherheitsforscher:innen vor ungerechtfertigter Strafverfolgung.

Das Problem liegt in der Ausgestaltung des § 118a StGB, da dieser auf die Absichten des:der Sicherheitsforscher:in abzielt. Diese sind im Regelfall nicht offensichtlich und müssen daher von den Strafverfolgungsbehörden auch entsprechend im Rahmen eines Ermittlungsverfahren geprüft werden (so wie in unserem Fall). Um dieser Unsicherheit und dem rechtlichen und finanziellen Risiko für die Aufdecker:innen von Sicherheitslücken vorzubeugen, schlagen wir vor, eine explizite gesetzliche Ausnahme für den verantwortlichen Umgang mit Sicherheitslücken zu schaffen, die unter gewissen Voraussetzung immer straffrei bleiben sollen. Genau für eine solche Regelung setzen wir uns seit Jahren[7] immer wieder[8] ein.

Warum reicht der Erlass des Justizministeriums nicht?

Im Erlass des Justizministerium zu diesem Thema[9] wird lediglich die ohnehin schon etablierte Rechtsmeinung nochmals dargelegt. Um ethische Sicherheitsforschung abzusichern bzw. zu fördern, bedarf es jedoch klarer gesetzlicher Ausnahmetatbestände, da sonst immer wieder ein Fall wie der unsrige auftreten kann.

---

3 Siehe dazu weiter unten „Wie machen es andere EU Staaten?"
4 siehe Tipold in Leukauf/Steininger, StGB4 § 118a Rz 8, Stand 1.10.2016
5 Vgl Seite 74 Report „Coordinated Vulnerability Disclosure Policies in the EU", ENISA, April 2022
6 https://ris.bka.gv.at/Dokumente/Erlaesse/ERL_BMJ_20230823_2023_0_603_326/ERL_BMJ_20230823_2023_0_603_326.pdf
7 https://epicenter.works/content/massive-sicherheitsluecke-in-oesterreich-testetat-aufgedeckt-gesundheitsministerium
8 https://epicenter.works/content/stellungnahme-zu-verschaerfungen-cyberkriminalitaet-begutachtungsverfahren
9 Siehe 2.2 https://ris.bka.gv.at/Dokument.wxe?ResultFunctionToken=b544b556-44b5-4d5a-a654-3ff6b14cefe4&Position=201&Sort=0%7cAsc&Abfrage=Erlaesse&Titel=&VonInkrafttretedatum=&BisInkrafttretedatum=&FassungVom=11.04.2023&Einbringer=&Abteilung=&Fundstelle=&GZ=&Norm=&ImRisSeitVonDatum=&ImRisSeitBisDatum=&ImRisSeit=Undefined&ImRisSeitForRemotion=Undefined&ResultPageSize=100&Suchworte=&Dokumentnummer=ERL_BMJ_20230823_2023_0_603_326

Wie machen es andere EU Staaten?

Auf EU-Ebene wurde diese Thematik durch die Agentur für Cybersicherheit („ENISA“) aufgegriffen[10] und es gibt eine ganz klare Empfehlung von dieser höchsten IT-Sicherheitsbehörde in Europa: Es braucht einen sicheren Rechtsrahmen für Sicherheitsforschung; das Melden von Sicherheitslücken darf nicht bestraft werden. ENISA vergleicht dabei auch die rechtliche Situation in den Mitgliedsländern und empfiehlt den EU-Staaten im Rahmen der Umsetzung der NIS2-Richtlinie so einen Rechtsrahmen zu schaffen. Die Umsetzung der NIS2-Richtlinie in Österreich lässt hier allerdings viel zu wünschen übrig.

Ein Vorreiter in dieser Hinsicht ist beispielsweise **Litauen**. Hier wurde insbesondere unter Federführung des Verteidigungsministeriums ein sicherer Rechtsrahmen für Sicherheitsforschung und den Umgang mit Sicherheitslücken geschaffen. Dabei spielten für Litauen besonders Überlegungen zu hybriden Bedrohungsszenarien aus Russland eine wichtige Rolle, was auch für Österreich keine unrealistischen Szenarien sind. Nach Anpassung der rechtlichen Rahmenbedingungen konnte so bereits im ersten Jahr nach Einführung eine Verdoppelung der gemeldeten Sicherheitslücken beim nationalen Cybersicherheitszentrum festgestellt werden.[11].

In den **Niederlanden** gibt es seit längerem eine diesbezügliche Praxis und dezidierte Förderprogramme.[12]

In **Deutschland** gibt es eine ähnliche legistische Situation wie in Österreich. Hier gab es in den letzten Jahren gleich zwei prominente Fälle, in denen völlig richtig handelnde Sicherheitsforscher:innen vor Gerichte gelandet sind. In einem Fall machte eine IT-Sicherheitsforscherin auf Sicherheitslücken in einer „Wahlapp“ einer wahlwerbenden Partei aufmerksam. Nach Anzeige gegen die Sicherheitsforscherin durch die von der Lücke betroffene Partei eröffnete die Staatsanwaltschaft ein Ermittlungsverfahren, welches jedoch schlussendlich eingestellt wurde.[13] In einem anderen Fall wurde sogar ein IT-Consultant zu einer vierstelligen Geldstrafe verurteilt[14], wobei der IT-Consultant jegliche kriminellen Absichten leugnet und diese Ansicht auch von Berichten einschlägiger Fachmedien gestützt wird.[15] Im Koalitionsabkommen der derzeitigen deutschen Bundesregierung findet sich immerhin das Bekenntnis: „Das Identifizieren, Melden und Schließen von Sicherheitslücken in einem verantwortlichen Verfahren, z. B. in der IT-Sicherheitsforschung, soll legal durchführbar sein“.[16]

Auf globaler Ebene wurde etwa ein Security Research Legal Defense Fund eingerichtet, getragen von renommierten Persönlichkeiten aus Forschung und Zivilgesellschaft. Er hat das Ziel, Sicherheitsforscher:innen und *Responsible-Disclosure*-Praktiken bei etwaigen Prozesskosten zu unterstützen.[17]

---

10 Vgl Seite 74 Report „Coordinated Vulnerability Disclosure Policies in the EU“, ENISA, April 2022

11 Siehe Seite 11,“Key trends and statistics of the national cyber security status of Lithuania 2021 – Q1 2022“, Ministry of National Defence of the Republic of Lithuania, abrufbar unter: https://www.nksc.lt/doc/en/Key-trends-and-statistics-2021-q1-2022.pdf

12 https://www.government.nl/topics/cybercrime/fighting-cybercrime-in-the-netherlands/responsible-disclosure

13 https://www.spiegel.de/netzwelt/netzpolitik/staatsanwaltschaft-bestaetigt-schwachstelle-in-wahlkampf-app-der-cdu-a-b66c2a32-4c4c-4337-83b3-795d749ee4b7

14 https://socket.dev/blog/ethical-hacking-on-trial-german-court-fines-security-researcher

15 Vgl https://www.heise.de/meinung/Kommentar-zu-Modern-Solution-Der-Staat-darf-kein-Handlanger-von-Stuempern-sein-6224293.html

16 Vgl Seite 13 des Koalitionsabkommens, abrufbar unter: https://www.spd.de/fileadmin/Dokumente/Koalitionsvertrag/Koalitionsvertrag_2021-2025.pdf

17 https://www.securityresearchlegaldefensefund.org/#what-we-do

Ist es mit einer Novellierung des § 118a StGB bereits getan?

Nein. Neben § 118a StGB gibt es noch eine Verwaltungsstrafbestimmung im Datenschutzgesetz (DSG), die einen ähnlichen Regelungsgehalt hat und darüber hinaus geeignet ist, Sicherheitsforschung und den verantwortlichen Umgang mit Sicherheitslücken zu bestrafen. Konkret handelt es sich dabei um § 62 Abs 1 Z 1 DSG. Demnach ist mit Geldstrafe bis zu 50.000 zu bestrafen, wer sich vorsätzlich widerrechtlich Zugang zu einer Datenverarbeitung verschafft oder einen erkennbar widerrechtlichen Zugang vorsätzlich aufrechterhält.

Hier sollte analog zu unserem Vorschlag zu § 118a StGB eine explizite rechtliche Ausnahme für den moralisch richtigen Umgang mit Sicherheitslücken geschaffen werden.

Was sollte man sonst noch tun?

Viele große Firmen[18] haben sogenannte „Bug Bounty Programme“[19]. Dabei werden öffentlich Preisgelder ausgelobt, wenn einem Unternehmen Sicherheitslücken in den eigenen Systemen gemeldet werden. Diese Preisgelder sind oft nur ein Bruchteil der Kosten, wenn bei IT-Firmen eine Überprüfung auf Sicherheitslücken beauftragt wird. Die Unternehmen sparen sich dadurch also Geld und Sicherheitsforscher:innen haben auf der anderen Seite die Sicherheit, dass sie bei Meldung einer Schwachstelle nicht strafrechtlich verfolgt werden. Für die Bevölkerung sind v.a. Sicherheitslücken im öffentlichen Bereich besonders gefährlich. Ihre Schließung ist daher besonders dringlich. Trotz dieser Dringlichkeit und der offensichtlichen Vorteile haben staatliche IT-Systeme in Österreich – mit ganz wenigen Ausnahmen[20] – keine Bug Bounty Programme. Wir schlagen daher vor, auch diese Möglichkeiten auszuschöpfen. Denn aktuell hinken wir in Sachen IT-Sicherheit anderen europäischen Staaten hinterher.

18 https://bughunters.google.com/about/rules/6625378258649088/google-and-alphabet-vulnerability-reward-program-vrp-rules und https://www.t-mobile.com/privacy-center/education/bug-bounty

19 https://www.security-insider.de/was-ist-ein-bug-bounty-programm-a-1052493/

20 https://www.verwaltungspreis.gv.at/Bug_Bounty_Programm