Legal and Technical Backround to the „EMS Scandal“

What criminal offence were we accused of specifically?

The accusation against epicenter.works was based on § 118a StGB "Unlawful access to a computer system" and also on the qualification of § 118a para. 2 StGB in relation to a computer system that is an essential component of the critical infrastructure (§ 74 para. 1 no. 11). We were thus faced with a penalty of up to two years' imprisonment.

It should be noted that § 118a StGB is a so-called enabling offence, meaning that prosecution can only take place if the injured party has given authorisation. In this case, this authorisation was granted by the responsible Minister of Health, Wolfgang Mückstein, and was not revoked by his successor, Health Minister Johannes Rauch, at our request.

Why was the prosecution discontinued?

Criminal liability under § 118a StGB only exists if the corresponding subjective elements of the offence are also fulfilled. These are given if:

1. intent to commit espionage: access to a computer system with the intention of obtaining knowledge of personal data for oneself or another unauthorised person. Knowledge of the data must violate the confidentiality interests of those affected that are worthy of protection.
2. intent to cause harm: a person is harmed by the use of the computer system or the data obtained from it.

Neither was present in this case. As a data protection organisation, we naturally obtained the consent of all persons whose data was accessed to verify the authenticity of the EMS in advance. There can therefore have been no intention to cause harm, as we merely verified the authenticity of a security vulnerability that was reported to us in order to have it closed immediately by those responsible. Our actions averted harm to those affected.

The objective elements of the offence were also not present, as we merely assessed and documented an existing security vulnerability as experts upon request by media.

What distinguishes the ethical handling of security vulnerabilities from computer crime?

Security research, which often takes place at universities or in government cybersecurity challenges, and computer criminals basically use the same methods and tools. Testing the security of a system is very often only possible by testing it for vulnerabilities. Whether a vulnerability really exists can only be tested by using it. When a locksmith tries to assess the security of a lock, he also tries to open it without a key.

The big difference between criminals and proper security researchers lies in how this vulnerability is handled. The concept of "Responsible Disclosure"[1] has been around for decades for the correct handling of security vulnerabilities. The security researcher reports the vulnerability to the manufacturer or responsible party so that this security gap can be closed. The vulnerability is only reported publicly once the threat has been eliminated. In many countries, there are legal safeguards for precisely this. Science demands it as well and the EU authority for IT security "ENISA" is also in favour of this.

If a security vulnerability is not reported and closed, it can also be exploited for attack purposes to cause damage or access data. Reporting, on the other hand, prevents this damage and improves security for everyone. Nevertheless, from reporting security vulnerabilities to manufacturers or those responsible, security researchers often not only cannot expect any advantage, but are often even threatened with criminal prosecution. (as in our case)

Why did it all take so long?

It is absolutely incomprehensible to us why **we were not informed about the complaint and the investigation proceedings against us for a year**. We should have been informed immediately. Apparently, the technical complexity of the proceedings was one reason why the investigating authorities were very slow to process the case. The first communication from the investigating authorities to us was also accompanied by a request to explain the (technical) facts of the case.

As soon as we were able to explain the facts of the case to the responsible public prosecutor in Innsbruck, he decided to discontinue the proceedings against us. However, the proceedings against us were combined with the proceedings against HG Lab Truck[2], as their careless handling had made this security breach possible in the first place. As a result, the entire case was categorised as a "clamorous proceeding" and had to be reported.

In proceedings subject to reporting, the responsible public prosecutor must first have every decision approved by the chain of command. This means that the senior public prosecutor's office and ultimately the Ministry of Justice must give their approval. So we had to wait **almost another year** until the proceedings against us were finally dropped, which cost us even more legal fees and nerves. Our lawyer Maria Windhager was informed by telephone that the proceedings had been discontinued. We are still waiting for the reasons for the discontinuation.

This was not an isolated case: why is a legal change needed?

Even though no charges were ultimately brought, the **costs of around EUR 15,000** and the time spent by epicenter.works were enormous. We believe that such expenditure could prevent independent security researchers, NGOs or journalists from investigating possible security vulnerabilities in the future or, once they have been closed, from reporting on them. The very behaviour that would serve the security of society as a whole and a democratic debate about realistic threat scenarios may therefore be penalised by the current legal situation, or at least made very unattractive by the high legal risk and the enormous effort involved. And this at a time when more and more countries and international organisations are beginning to understand the added value that security research can generate for the general public and cyber security in particular.[3]

1 https://en.wikipedia.org/wiki/Coordinated_vulnerability_disclosure
2 https://www.derstandard.at/story/2000133001435/erste-klagen-wegen-datenleck-bei-hg-lab-truck-eingebracht
3 See below "How do other EU countries do it?"

It should also be noted that the offence of § 118a of the Austrian Criminal Code (StGB) is very rarely applied, especially as the substantiation of evidence is extremely difficult. However, this makes it particularly easy for security researchers, who would deliberately pass on information about the security vulnerability to those responsible and thus improve protection against attacks, to be targeted by investigations. This leads to the paradoxical situation that, from the security researchers' point of view, ethical behaviour is "punished" and thus the overarching legal policy objective pursued by § 118a StGB is not achieved: namely protection against IT attacks (the "unlawful access of a computer system").

What do the scientific community and the Ministry of Justice have to say about this?

The fact that security research that adheres to responsible disclosure rules should not actually fall under the criminal offence of § 118a StGB has long been advocated by the scientific community[4][5]. Since August 2023, there has also been a corresponding decree[6] from the Ministry of Justice. However, this legal opinion in itself does not protect security researchers who act correctly from unjustified prosecution.

The problem lies in the design of § 118a StGB, as it is aimed at the intentions of the security researcher. Generally these are not obvious and must therefore be examined accordingly by the law enforcement authorities as part of an investigation (as happened in our case). In order to prevent this uncertainty and the legal and financial risk for those who uncover security vulnerabilities, we propose creating an explicit legal exception for the responsible handling of security vulnerabilities, which should always remain exempt from prosecution under certain conditions. This is precisely the kind of regulation we have been repeatedly[7] advocating for years[8].

Why is the Ministry of Justice's decree not enough?

The Ministry of Justice's decree on this topic[9] merely restates the already established legal opinion. In order to safeguard and promote ethical security research, however, clear legal exceptions are required, as otherwise a case like ours could arise again multiple times.

4 See Tipold in Leukauf/Steininger, StGB4 § 118a Rz 8, as of 1 October 2016
5 Compare page 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 See 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

How do other EU countries do it?

At EU level, this issue has been taken up by the Agency for Cybersecurity ("ENISA")[10] and there is a very clear recommendation from this highest IT security authority in Europe: there needs to be a secure legal framework for security research; reporting security vulnerabilities must not be penalised. ENISA also compares the legal situation in the member states and recommends that the EU states create such a legal framework as part of the implementation of the NIS2 Directive. However, the implementation of the NIS2 Directive in Austria leaves a lot to be desired.

Lithuania, for example, is a pioneer in this regard. Here, a secure legal framework for security research and the handling of security vulnerabilities was created under the leadership of the Ministry of Defence. Considerations regarding hybrid threat scenarios from Russia played a particularly important role for Lithuania, which are no unrealistic scenarios for Austria either. After adapting the legal framework, the number of security breaches reported to the national cyber security centre doubled in the first year after introduction[11].

In the Netherlands, there has long been a practice in this regard and dedicated support programmes exist.[12]

The legal situation in Germany is similar to that in Austria. There have been two prominent cases here in recent years in which security researchers who acted correctly ended up in court. In one case, an IT security researcher drew attention to security vulnerabilities in an "election app" of a campaigning party. After the party affected by the vulnerability filed a complaint against the security researcher, the public prosecutor's office opened an investigation, which was ultimately dropped.[13] In another case, an IT consultant was even sentenced to a four-figure fine[14], although the IT consultant denies any criminal intent and this view is also supported by reports in the relevant specialist media.[15] The coalition agreement of the current German government does include the commitment: "Identifying, reporting and closing security gaps in a responsible process, e.g. in IT security research, should be legally feasible".[16]

At the global level, a Security Research Legal Defence Fund has been set up, supported by renowned figures from research and civil society. Its aim is to support security researchers and responsible disclosure practices in the event of legal costs.[17]

Is an amendment to § 118a StGB enough?

No. In addition to § 118a StGB, there is also an administrative offence provision in the Data Protection Act (DSG, Datenschutzgesetz) that has a similar regulatory content and is also suitable for punishing

10 See page 74 Report "Coordinated Vulnerability Disclosure Policies in the EU", ENISA, April 2022
11 See page 11, "Key trends and statistics of the national cyber security status of Lithuania 2021 - Q1 2022", Ministry of National Defence of the Republic of Defence of the Republic of Lithuania, available at: 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 Compare https://www.heise.de/meinung/Kommentar-zu-Modern-Solution-Der-Staat-darf-kein-Handlanger-von-Stuempern-sein-6224293.html
16 Compare page 13 of the coalition agreement, available at: https://www.spd.de/fileadmin/Dokumente/Koalitionsvertrag/Koalitionsvertrag_2021-2025.pdf
17 https://www.securityresearchlegaldefensefund.org/#what-we-do

security research and the responsible handling of security vulnerabilities. Specifically, this is § 62 para. 1 no. 1 DSG. According to this, anyone who wilfully obtains illegal access to data processing or wilfully maintains recognisably illegal access is liable to a fine of up to 50,000€.

In analogy to our proposal for § 118a StGB, an explicit legal exception should be created for the morally correct handling of security vulnerabilities.

What else should be done?

Many large companies[18] have so-called "bug bounty programmes"[19], where public prizes are awarded if a company is notified of security vulnerabilities in its own systems. These prizes are often only a fraction of the cost of commissioning IT companies to check for security vulnerabilities.This saves companies money and, on the other hand, gives security researchers the certainty that they will not be prosecuted if they report a vulnerability. Security vulnerabilities in the public sector are particularly dangerous for the general public. Closing them is therefore particularly urgent. Despite this urgency and the obvious advantages, government IT systems in Austria - with very few exceptions[20] - do not have bug bounty programmes. We therefore suggest that these possibilities should also be utilised. After all, we are currently lagging behind other European countries in terms of IT security.

18 https://bughunters.google.com/about/rules/6625378258649088/google-and-alphabet-vulnerability-reward-program-vrp-rules and 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