WIEN / 19. April 2023

Stellungnahme zu Verschärfungen Cyberkriminalität

Begutachtungsverfahren zum Ministerialentwurf betreffend Strafgesetzbuch und Bundesgesetz gegen den unlauteren Wettbewerb 1984 – UWG, Änderung

(Geschäftszahl: 253/ME)

Für epicenter.works
Thomas Lohninger
Dominik Polakovics
Walter Hötzendorfer
Tanja Fachathaler

EPICENTER .WORKS
for digital rights

VORWORT UND KURZFASSUNG

Wir bedanken uns für die Möglichkeit, im Begutachtungsverfahren[1] folgende Stellungnahme abgeben zu können. Wir beschränken uns in dieser Stellungnahme großteils auf die Bestimmung des Widerrechtlichen Zugriffs auf ein Computersystem und zeigen auf, wieso die vorgeschlagene Bestimmung negative Auswirkungen auf die Sicherheit von Computersystemen in Österreich haben kann.

Inhaltsverzeichnis

1 https://www.parlament.gv.at/gegenstand/XXVII/ME/253?selectedStage=100

WIDERRECHTLICHER ZUGRIFF AUF EIN COMPUTERSYSTEM (§ 118A)

Allgemeine Ausführungen

Wie Sicherheitslücken gefunden werden

Unabhängig von den Anstrengungen der Verantwortlichen ist davon auszugehen, dass jedes Computersystem Sicherheitslücken aufweist. Das Schließen dieser Sicherheitslücken ist Teil der Sorgfaltspflichten der Verantwortlichen für die Datenverarbeitung gemäß Art 32 DSGVO und dem künftigen Cyber Resilience Act (CRA) 2022/0272(COD). Oftmals sind es jedoch nicht die Verantwortlichen für das Computersystem selbst, welche diese Sicherheitslücken auffinden. In vielen Fällen sind es unabhängige Sicherheitsforscher:innen, die diese Lücken entdecken und dann vor einer schwierigen Entscheidung stehen, insbesondere wenn die Motive ihres Handelns im Sinne der Allgemeinheit sind.

Oftmals sind es nicht die Mitarbeiter:innen des Verantwortlichen für die Datenverarbeitung oder des Herstellers des IT-Systems, die diese Sicherheitslücken bemerken. Nur ein kleiner Teil der unabhängigen Sicherheitsforschung, die weltweit und auch in Österreich betrieben wird, wird im Vorhinein durch die Verantwortlichen oder Hersteller der jeweiligen Systeme autorisiert. Der Zugriff auf personenbezogene Daten ist dabei häufig nicht vermeidbar. Dadurch setzt sich legitime und gesellschaftlich äußerst wertvolle Sicherheitsforschung regelmäßig der Gefahr strafrechtlicher Verfolgung gemäß § 118a aus, sodass eine Erhöhung der Strafdrohung ohne entsprechende Ausnahmeregelung für legitime Sicherheitsforschung als hochproblematisch anzusehen ist.[2]

Die drei Arten mit Sicherheitslücken umzugehen

Sicherheitsforscher:innen könnten ihr Wissen über Sicherheitslücken in operativen Computersystemen in vielen Fällen leicht zu Geld machen, wofür leider ein lebendiger Schwarzmarkt an Sicherheitslücken und verwundbaren Systemen besteht. Teils werden auf diesen Schwarzmärkten sehr hohe Preise für derartiges Wissen erzielt.

Wenn Sicherheitsforscher:innen stattdessen den Weg wählen, die Verantwortlichen bzw. Hersteller:innen zu informieren, damit die Sicherheitslücke geschlossen wird, setzen sie sich der Gefahr von zivil- und strafrechtlichen Konsequenzen aus, wobei die gegenständliche Bestimmung derzeit ein Hauptproblem darstellt. In Verbindung mit der Veröffentlichung von Sicherheitslücken nachdem dem Verantwortlichen bzw. dem/der Hersteller:in eine angemessene Frist zur Behebung eingeräumt wurde, bezeichnet man dieses Vorgehen als „responsible disclosure".[3] Durch die Veröffentlichung nachdem die Gefahr gebannt wurde, wird ein informierter Diskurs über die Sicherheit wichtiger Computersysteme und der Verantwortung von Hersteller:innen erst ermöglicht. Obwohl responsible disclosure das moralisch korrekte Handeln im Sinne der Allgemeinheit darstellt, gibt es aktuell keinerlei Anreize staatlicherseits für dieses Vorgehen.

2 Zwar schränkt der in Abs 1 leg cit normierte erweiterte Vorsatz die Bestimmung ein, dies wird aber häufig nicht die Einleitung eines Strafverfahrens verhindern und die Beweisführung in Bezug auf die innere Tatseite ist schwierig und mit entsprechender Unsicherheit verbunden.

3 https://de.wikipedia.org/wiki/Responsible_Disclosure_(IT-Sicherheit)

Unter der aktuellen Rechtslage entscheiden sich viele Sicherheitsforscher:innen deshalb dazu, die Kenntnis über Sicherheitslücken in operativen Systemen entweder für sich zu behalten oder anonym zu veröffentlichen, während die Sicherheitslücke noch aufrecht ist. Durch dieses Vorgehen wird die Sicherheit der betroffenen Computersysteme unterminiert und es entsteht eine Gefahr für die Betroffenen.

Weiters gibt es derzeit keinerlei Verpflichtungen für Hersteller:innen, mit Sicherheitsforscher:innen zusammen zu arbeiten, um Lücken zu schließen oder zumindest auf etwaige Meldungen von Sicherheitslücken zu reagieren, erst recht nicht wenn diese anonym erfolgen. Wir hoffen auf eine diesbezügliche Verbesserung in den laufenden Verhandlungen zum CRA.

Anreiz für korrektes Handeln

Die derzeitige Rechtslage setzt Anreize entgegen der Steigerung der Sicherheit von IT-Systemen. Viele Unternehmen reagieren negativ auf das Aufzeigen von Schwachstellen in ihren Systemen. Anstatt im Sinne der Sicherheit Lücken schnellstmöglich zu schließen, werden oftmals die Sicherheitsforscher:innen angezeigt. Dieses Problem setzt sich fort bei der Meldung von Sicherheitslücken in staatlichen Systemen. Hier sind die Zuständigen oft verpflichtet, Meldungen von Schwachstellen zur Anzeige zu bringen und erteilen gleichsam oft die Autorisierung zur Strafverfolgung, um einer Amtshaftung zu entgehen.

Vor diesem Hintergrund erscheint der Verweis auf die COVID-19-Pandemie in den Erläuterungen als Hohn, wo doch genau in dieser Krisenzeit eine Vielzahl von Sicherheitslücken in staatlichen Systemen aufgedeckt wurden und die Reaktion von staatlicher Seite oft ein Angriff auf die Sicherheitsforscher:innen war.[4] In mehreren Fällen konnte Schaden für die Sicherheitsforscher:innen nur deshalb abgewendet werden, weil die Sicherheitslücken noch vor Inbetriebnahme der Systeme aufgrund von Leaks der Systembeschreibung und Open-Source-Prüfungen entdeckt wurden[5].

Lösungsvorschläge

Wir schlagen eine Neufassung des §118a vor, die eine Verhältnismäßigkeitsprüfung der Strafbarkeit im Hinblick auf Handeln im Sinne der öffentlichen Sicherheit vorsieht. In einer solchen Lösung käme es auf den Umgang mit einer Sicherheitslücke an, sodass ein im oben beschriebenen Sinne verantwortungsvoller Umgang mit diesem kritischen Wissen über Sicherheitslücken den handelnden Personen nicht mehr nachteilig ausgelegt werden kann. Nach diesem Vorschlag wäre eine Prüfung der Verhältnismäßigkeit zwischen dem abgewendeten und realisierten Schaden herzustellen, wobei auf die Absicht der Tat bedacht genommen wird, sodass jedes tatsächlich schädigende Handeln weiterhin strafbar bleibt.

Dazu schlagen wir folgende konkrete Formulierung vor:

> „Der Täter ist nicht zu bestrafen, wenn er sich zu dem Computersystem nur in der Absicht Zugang verschafft, dessen Sicherheit zu analysieren, und die von ihm angewendete Methode zur Überwindung der spezifischen Sicherheitsvorkehrung dem Betreiber des Computersystems binnen angemessener Frist meldet."

Sollte dies politisch nicht realisierbar sein, wäre zumindest eine Möglichkeit einer zivil- oder strafrechtlichen Immunität für Sicherheitsforschung mit verantwortungsvollem Umgang mit

4 https://epicenter.works/content/massive-sicherheitsluecke-in-oesterreich-testetat-aufgedeckt-gesundheitsministerium

5 https://epicenter.works/content/sicherheitsluecken-im-gruenen-pass-gefaehrden-gesundheitsdaten-aller-sozialversicherten und https://epicenter.works/content/analyse-der-stopp-corona-app-des-roten-kreuzes

Sicherheitslücken vorzusehen, wie dies in Belgien der Fall ist[6]. Im Kontrast zum belgischen Modell sollte jedoch auch eine Meldung nicht nur an eine staatliche Stelle, sondern analog zur Hinweisgeber-Richtlinie der EU auch an die Verantwortlichen der betroffenen Computersysteme möglich sein. In jedem Fall sollte eine Veröffentlichung der Sicherheitslücke nach deren Reparatur nicht ausgeschlossen werden, sondern nach einer verhältnismäßigen Zeit den Sicherheitsforschenden als Option zur Verfügung stehen.

Zuletzt wäre zumindest ein Erlass des Bundesministers für Kunst, Kultur, öffentlichen Dienst und Sport anzuregen, um der Anzeige von gemeldeten Sicherheitslücken und einer Autorisierung der Strafverfolgung gegen im öffentlichen Interesse handelnden Sicherheitsforscher:innen abzusehen, wie dies in den Niederlanden auf der Ebene der Staatsanwaltschaft mit der Abkehr von Strafverfolgung in derartigen Fällen gängige Praxis ist[7]. Diese Lösung würde lediglich staatliche Systeme betreffen und ist deshalb nicht hinreichend.

SONSTIGE BESTIMMUNGEN

Wir begrüßen die Änderungen in §119, §119a, §121 aus Sicht des Datenschutzes.

Wir kritisieren die fehlende Trennschärfe des §126c im Bezug auf gängige Open-source-Werkzeuge in der Sicherheitsforschung, welche oftmals sowohl zum Austesten von Schwachstellen für autorisierte Sicherheitsprüfungen, wie auch für kriminelle Absichten verwendet werden können.[8]

6 https://ccb.belgium.be/en/vulnerability-reporting-ccb

7 https://www.om.nl/onderwerpen/cybercrime/coordinated-vulnerability-disclosure---ethisch-hacken ; https://www.om.nl/onderwerpen/cybercrime/documenten/brochures/cybercrime/2018/oktober/coordinated-vulnerability-disclosure-de-leidraad

8 Siehe z.B. https://de.wikipedia.org/wiki/Metasploit