RUHR-UNIVERSITÄT BOCHUM

RUB

RUBIN

WISSENSCHAFTSMAGAZIN

GEHEIMNIS

Auf Blei: Verflucht im Römischen Reich

In den Genen: Vererbte Krankheiten

Zwischen den Zeilen: Versteckte Botschaften

#35 Nr. 1 | 2025

Datei Bearbeiten Ansicht Suchen Terminal Hilfe
[0.449458] kernel: pci 0000:64:0d.0: [8086:2048] type 00 class 0x088000 PCIe Root Complex Integrated Endpoi
[0.449544] kernel: pci 0000:64:0d.1: [8086:2049] type 00 class 0x088000 PCIe Root Complex Integrated Endpoi
[0.449612] kernel: pci 0000:64:0d.2: [8086:204a] type 00 class 0x088000 PCIe Root Complex Integrated Endpoi
[0.449679] kernel: pci 0000:64:0d.3: [8086:204b] type 00 class 0x088000 PCIe Root Complex Integrated Endpoi
[0.449798] kernel: pci 0000:65:00.0: [10de:1f82] type 00 class 0x030000 PCIe Legacy Endpoint
[0.449815] kernel: pci 0000:65:00.0: BAR 0 [mem 0xd7000000-0xd7ffffff]
[0.449831] kernel: pci 0000:65:00.0: BAR 1 [mem 0xc0000000-0xcfffffff 64bit pref]
[0.449847] kernel: pci 0000:65:00.0: BAR 3 [mem 0xd0000000-0xd1ffffff 64bit pref]
[0.449859] kernel: pci 0000:65:00.0: BAR 5 [io 0xb000-0xb07f]
[0.449869] kernel: pci 0000:65:00.0: ROM [mem 0xd8000000-0xd807ffff pref]
[0.449874] kernel: pci 0000:65:00.0: enabling Extended Tags
[0.449900] kernel: pci 0000:65:00.0: Video device with shadowed ROM at [mem 0x000c0000-0x000dffff]
[0.449932] kernel: pci 0000:65:00.0: PME# supported from D0 D3hot D3cold
[0.449987] kernel: pci 0000:65:00.0: 32.000 Gb/s available PCIe bandwidth, limited by 2.5 GT/s PCIe x16 li
[0.450083] kernel: pci 0000:65:00.1: [10de:10fa] type 00 class 0x040300 PCIe Endpoint
[0.450100] kernel: pci 0000:65:00.1: BAR 0 [mem 0xd8080000-0xd8083fff]
[0.450160] kernel: pci 0000:65:00.1: enabling Extended Tags
[0.450252] kernel: pci 0000:64:00.0: PCI bridge to [bus 65]
[0.450265] kernel: pci_bus 0000:64: on NUMA node 0
[0.450433] kernel: ACPI: PCI Root Bridge [PC03] (domain 0000 [bus b2-ff])
[0.450437] kernel: acpi PNP0A08:03: _OSC: OS supports [ExtendedConfig ASPM ClockPM Segments MSI EDR HPX-
[0.450824] kernel: acpi PNP0A08:03: _OSC: platform does not support [SHPCHotplug AER LTR DPC]
[0.451135] kernel: acpi PNP0A08:03: _OSC: OS now controls [PCIeHotplug PME PCIeCapability]
[0.451331] kernel: PCI host bridge to bus 0000:b2
[0.451333] kernel: pci_bus 0000:b2: root bus resource [io 0xc000-0xffff window]
[0.451335] kernel: pci_bus 0000:b2: root bus resource [mem 0xd9000000-0xfbffffff window]
[0.451336] kernel: pci_bus 0000:b2: root bus resource [bus b2-ff]
[0.451348] kernel: pci 0000:b2:05.0: [8086:2034] type 00 class 0x088000 PCIe Root Complex Integrated En
[0.451432] kernel: pci 0000:b2:05.2: [8086:2035] type 00 class 0x088000 PCIe Root Complex Integrated En
[0.451514] kernel: pci 0000:b2:05.4: [8086:2036] type 00 class 0x080020 PCIe Root Complex Integrated En
[0.451528] kernel: pci 0000:b2:05.4: BAR 0 [mem 0xfbf00000-0xfbf00fff]
[0.451623] kernel: pci 0000:b2:12.0: [8086:204c] type 00 class 0x110100 PCIe Root Complex Integrated En
[0.451707] kernel: pci 0000:b2:12.1: [8086:204d] type 00 class 0x110100 conventional PCI endpoint
[0.451763] kernel: pci 0000:b2:12.2: [8086:204e] type 00 class 0x088000 conventional PCI endpoint
[0.451820] kernel: pci 0000:b2:15.0: [8086:2018] type 00 class 0x088000 conventional PCI endpoint
[0.451896] kernel: pci 0000:b2:16.0: [8086:2018] type 00 class 0x088000 conventional PCI endpoint
[0.451968] kernel: pci 0000:b2:16.4: [8086:2018] type 00 class 0x088000 conventional PCI endpoint
[0.452025] kernel: pci 0000:b2:17.0: [8086:2018] type 00 class 0x088000 conventional PCI endpoint
[0.452098] kernel: pci_bus 0000:b2: on NUMA node 0
[0.452389] kernel: ACPI: PCI: Interrupt link LNKA configured for IRQ 11
[0.452452] kernel: ACPI: PCI: Interrupt link LNKB configured for IRQ 10
[0.452514] kernel: ACPI: PCI: Interrupt link LNKC configured for IRQ 14
[0.452576] kernel: ACPI: PCI: Interrupt link LNKD configured for IRQ 15
[0.452638] kernel: ACPI: PCI: Interrupt link LNKE configured for IRQ 3
[0.452700] kernel: ACPI: PCI: Interrupt link LNKF configured for IRQ 5
[0.452760] kernel: ACPI: PCI: Interrupt link LNKG configured for IRQ 6
[0.452822] kernel: ACPI: PCI: Interrupt link LNKH configured for IRQ 11
[0.453044] kernel: ACPI: EC: interrupt unblocked
[0.453045] kernel: ACPI: EC: event unblocked
[0.453050] kernel: ACPI: EC: EC_CMD/EC_SC=0x66, EC_DATA=0x62
[0.453051] kernel: ACPI: EC: GPE=0x16
[0.453052] kernel: ACPI: _SB_.PC00.LPC0.EC0_: Boot DSDT EC initialization complete
[0.453054] kernel: ACPI: _SB_.PC00.LPC0.EC0_: EC: Used to handle transactions and events
[0.453758] kernel: iommu: Default domain type: Translated
[0.453758] kernel: iommu: DMA domain TLB invalidation policy: lazy mode
[0.453899] kernel: SCSI subsystem initialized
[0.453905] kernel: libata version 3.00 loaded.
[0.453905] kernel: ACPI: bus type USB registered
[0.453905] kernel: usbcore: registered new interface driver usbfs
FUJITSU

Strafrecht

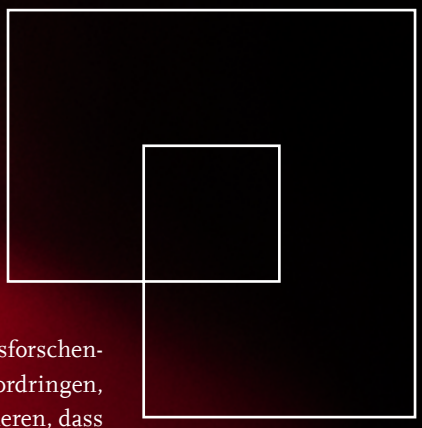
GESETZLICH GESCHÜTZTE GEHEIMNISSE

Mit elf wurde Sebastian Golla beim Hacken erwischt und fing Feuer für das Thema. Heute setzt er sich als Jurist dafür ein, dass Forschende, die Sicherheitslücken aufdecken, vor Strafverfolgung geschützt werden.

Geheimnisse bewahren im virtuellen Raum – keine leichte Aufgabe. Im Interview spricht Prof. Dr. Sebastian Golla über Grauzonen und Lücken im IT-Strafrecht. Außerdem schlägt der Jurist Regelungen vor, die es IT-Sicherheitsforschenden und Behörden erleichtern würden, unsere Daten zu schützen.

Herr Professor Golla, wie ist im deutschen Recht der Schutz von Geheimnissen, etwa von privaten Daten, geregelt?
Der Schutz von Geheimnissen ist eine Querschnittsmaterie und wird an unterschiedlichen Stellen, im Zivilrecht, öffentlichen Recht und Strafrecht geregelt. So gibt es beispielsweise ein Gesetz zum Schutz von Geschäftsgeheimnissen. Dieses zielt vor allem darauf, dass Geheimnisse im Wettbewerb geschützt sind. Oder denken wir an Verschwiegenheitspflichten für bestimmte Berufsgruppen – auch dieser Schutz ist gesetzlich geregelt.

Ihr Forschungsgebiet umfasst das Strafrecht – wo ist hier der Geheimnisschutz verankert?
Im Strafrecht gibt es verschiedene Regelungen, die Geheimnisse schützen beziehungsweise den Bruch von Geheimnissen unter Strafe stellen. Das Strafgesetzbuch ist so strukturiert, dass es neben dem Allgemeinen Teil, der für alle Straftaten gilt, zahlreiche Abschnitte gibt, die sich auf bestimmte Typen von Straftaten beziehen. Ein Schutz von Geheimnissen findet sich unter anderem im Abschnitt über die Verletzung des persönlichen Lebens- und Geheimbereichs. Dort geregelt sind unter anderem Delikte zum Schutz der Vertraulichkeit von Daten, auf die ich mich zuletzt spezialisiert habe.



Wenn IT-Sicherheitsforschende in ein System vordringen, dann kann es passieren, dass sie Zugangsbarrieren überwinden und den Zugriff auf Daten erlangen, die eigentlich nicht für sie vorgesehen sind. Und das steht unter Strafe.

Wie gut sind wir in Deutschland im Bereich IT-Strafrecht aufgestellt?
Deutschland ist eigentlich recht fortschrittlich in diesem Bereich. Wir haben in den 1980er-Jahren schon Straftatbestände verabschiedet, die bis heute Geltung haben. Und auch in den internationalen Ermittlungen waren wir immer weit vorne mit dabei.

Wo sehen Sie Verbesserungsbedarf?
Das IT-Strafrecht bleibt ein Gebiet des Strafrechts, in dem man gesetzlich noch viel Grundsätzliches festhalten und sehr viel verbessern kann. Ich wünsche mir vor allem ein konsistentes, kriminologisch fundiertes System von Strafbarkeit für den virtuellen Bereich. Verbesserungsbedarf sehe ich konkret zum Beispiel im Bereich der virtuellen Kommunikation, Stichwort Hate Speech, und auch im Bereich der IT-Sicherheitsforschung.

An der Ruhr-Universität Bochum wird viel zum Thema IT-Sicherheit geforscht. Inwiefern können unsere Forschenden mit dem Strafrecht in Berührung kommen?
Das IT-Strafrecht gewährleistet, dass unsere Computersysteme und Daten geschützt sind. Die Verletzung ihrer Integrität ist unter Strafe gestellt. Forschende, die im Bereich der IT-Sicherheit unterwegs sind, wollen ebenfalls zum Schutz der IT-Systeme und Software beitragen. Dafür klopfen sie unter anderem Systeme ab und testen, ob diese resilient sind. Wenn sie also explorativ in eine freie Umgebung reingehen und versuchen, in ein System vorzudringen, dann kann es passieren, dass sie Zugangsbarrieren überwinden und den Zugriff auf Daten erlangen, die eigentlich nicht für sie vorgesehen sind. Und das steht unter Strafe. ▸

Der Paragraf 202a des Strafgesetzbuchs, umgangssprachlich Hackerparagraf genannt, bedroht das unbefugte Ausspähen von Daten mit bis zu drei Jahren Freiheitsstrafe.

Sebastian Golla ist Juniorprofessor für Kriminologie, Strafrecht und Sicherheitsforschung im digitalen Zeitalter. Seine Forschung zeigt, dass die geltende Rechtslage im IT-Strafrecht unbefriedigend ist.

> „DEUTSCHLAND IST EIGENTLICH RECHT FORTSCHRITTLICH IM BEREICH IT-STRAFRECHT.“
>
> Sebastian Golla

Wie lautet der konkrete Strafbestand?
Konkret geht es um den Paragrafen 202a des Strafgesetzbuchs, umgangssprachlich Hackerparagraf genannt. Dieser bedroht das unbefugte Ausspähen von Daten mit bis zu drei Jahren Freiheitsstrafe und setzt voraus, dass man sich Daten verschafft oder auf Daten zugreift, die durch technische Vorkehrungen vor dem Zugriff besonders geschützt sind. Das ist ein relativ schlecht formulierter Tatbestand. Allein der Begriff „Daten“ ist zum Beispiel sehr vage definiert. Und der sogenannte formelle Geheimnisschutz besteht bereits, wenn man die Daten mit einer leichten Zugangsbarriere, etwa dem Passwort 12345, versieht.

Gibt es Fälle, in denen aufgrund dieses Tatbestands bereits Anklage gegen Forschende erhoben wurde?
Der bekannteste Fall aus Deutschland ist der von Lilith Wittmann. Wittmann hat 2021 in der Wahlkampf-App CDU connect eine Sicherheitslücke aufgedeckt – die Daten waren öffentlich zugänglich. Die CDU erstattete erst Strafanzeige, zog diese später zurück. Das Verfahren wurde eingestellt. Dieser Fall ist deswegen für Forschende interessant, weil Aktivist*innen wie Wittmann nicht ohne wissenschaftliche Fundierung arbeiten. Auch wenn in diesem Fall keine Anklage erhoben wurde, sind die Einschüchterungseffekte nicht zu vernachlässigen. Wenn jemand um sechs Uhr morgens bei Ihnen klingelt und alle Ihre technischen Geräte beschlagnahmt, dann macht das etwas mit Ihnen.

Wie kann man gutwillige IT-Sicherheitsforschung schützen?
Mein Kollege Dominik Brodowski und ich haben dazu einen Sammelband herausgegeben, in dem wir mehrere juristische Möglichkeiten diskutieren. Eine Option ist es, Forschungstätigkeiten zum Aufspüren von Sicherheitslücken von vornherein vom Tatbestand auszuschließen. Das ist die von uns bevorzugte Lösung. Eine andere ist es, zu sagen, dass das Forschungsverhalten zwar grundsätzlich vom Straftatbestand erfasst wird, aber als gerechtfertigt angesehen wird. Im Strafrecht haben wir in vielen Situationen diese Konstellation, etwa wenn es um Notwehr oder Nothilfe geht. Und dann gibt es noch die tätige Reue im Strafrecht. Wenn man sich im Nachgang einer Tat sofort eines Besseren besinnt und die schädlichen Folgen rückgängig macht, lässt sich die Strafe reduzieren oder ausschließen.

Wie reagieren Forschung und Politik auf Ihre Vorschläge?
Die IT-Sicherheitsforschung interessiert sich sehr dafür. Das sieht man auch daran, dass sich deutschlandweit praktisch sämtliche relevanten Forschungseinrichtungen zu dem Thema positioniert haben. Auch hier an der Ruhr-Universität Bochum ist das Interesse an rechtlichen Fragen groß. Das merke ich in meinen Lehrveranstaltungen zu dem Thema, an denen auch Interessierte aus der Informatik und den IT Security Studies teilnehmen.

Auch mit Politikschaffenden haben wir hier in Bochum viel diskutiert. Und tatsächlich stand im Koalitionsvertrag, dass die IT-Sicherheitsforschung entkriminalisiert werden soll. Im vergangenen November wurde ein Entwurf vorgelegt, der konkret vorschlug, das Gesetz so zu formulieren, dass Tätigkeiten mit der Absicht, Sicherheitslücken aufzudecken, von der Strafbarkeit ausgenommen sind. Dieses fällt jetzt höchstwahrscheinlich dem Koalitionsbruch zu Opfer. Ich hoffe dennoch, dass die gesetzliche Klarstellung bald kommt.

Und bis dahin? Was machen Forschende im Falle einer Anklage?
Man muss das Ganze freihändig lösen. Es gibt in dem Tatbestand ein paar Stellschrauben, an denen man drehen kann. Es gibt zum Beispiel das Merkmal, dass man den Zugriff auf Daten unbefugt erhalten haben muss. Man könnte eine Befugnis herleiten, nach der die Forschungstätigkeit adäquat war und einem legitimen Interesse diente. Das ist jedoch nicht trivial.

Ich nehme an, dass derzeit Fälle, in denen eine Forschungseinrichtung mit einem seriösen Anliegen hinter einem unbefugten Daten-Zugriff steht, über die zuständigen Staatsanwaltschaften lokal gelöst werden. Das wird aber nicht öffentlich kommuniziert.

Doch dass man in solchen Graubereichen irgendwie eine informelle Lösung findet – darauf können wir uns im Rechtsstaat nicht immer verlassen. Es muss klare Regeln geben. Und das ist eigentlich gar nicht so ein Hexenwerk.

Text: lb, Fotos: tk

REDAKTIONSSCHLUSS

Schon im 15. Jahrhundert dachten sich die Menschen trickreiche Lösungen aus, um Geheimnisse sicher weitergeben zu können, zum Beispiel die rechts abgebildete Chiffrierscheibe (mehr dazu ab Seite 26). Mit ihr konnte man einen Klartext in Kauderwelsch verwandeln, indem man die Buchstaben des Klartextes auf dem äußeren Ring durch die Buchstaben auf dem inneren Ring ersetzte. Der innere Ring war drehbar. Um einen verschlüsselten Text zu entschlüsseln, musste man wissen, wie der innere Ring auszurichten ist. Die Ausrichtung wurde von sogenannten Steuerungsbuchstaben bestimmt, also Buchstaben, die keine Entsprechung im Klartext hatten, sondern nur dazu bestimmt waren, die Ausrichtung des inneren Rings anzugeben. War dieser richtig gedreht, konnte man den Klartext auf dem äußeren Ring ablesen.

LUST ZU KNOBELN?

Dann inneren Ring der Scheibe ausschneiden und los geht's:

yuose&azmydbkofxczn&cdeuqmlitokhyds

Hinweise: Unser Beispiel ergibt einen Satz mit sechs Wörtern und beinhaltet acht Steuerungsbuchstaben. Steuerungsbuchstaben müssen auf das Z des äußeren Rings ausgerichtet werden. Der verschlüsselte Text in diesem Beispiel beginnt mit einem Steuerungsbuchstaben. Die anderen sieben Steuerungsbuchstaben sind zufällig im Text verteilt und können auch mitten im Wort auftreten. Immer wenn ein Zeichen aus unserem Kauderwelsch-Beispiel sich nicht in einen sinnvollen Buchstaben übersetzen lässt, handelt es sich um einen Steuerungsbuchstaben. Richten Sie dann den inneren Ring neu aus, indem Sie dieses Zeichen des inneren Rings auf das große Z des äußeren Rings drehen. Achtung: Da der Erfinder der Chiffrierscheibe Latein sprach, fehlt der Buchstabe U im äußeren Ring, der für unseren Lösungssatz erforderlich ist. Ein V im äußeren Ring kann sowohl ein U als auch ein V bedeuten. Viel Spaß!

Die Auflösung finden Sie unten links auf dieser Seite.

IMPRESSUM

HERAUSGEBER: Rektorat der Ruhr-Universität Bochum in Verbindung mit dem Dezernat Hochschulkommunikation der Ruhr-Universität Bochum (Hubert Hundt, v.i.S.d.P.)

WISSENSCHAFTLICHER BEIRAT: Prof. Dr. Birgit Apitzsch (Sozialwissenschaft), Prof. Dr. Thomas Bauer (Fakultät für Wirtschaftswissenschaft), Prof. Dr. Elena Enax-Krumova (Medizin), Prof. Dr. Constantin Goschler (Geschichtswissenschaften), Prof. Dr. Markus Kaltenborn (Jura), Prof. Dr. Achim von Keudell (Physik und Astronomie), Prof. Dr. Günther Meschke (Prorektor für Forschung und Transfer), Prof. Dr. Martin Muhler (Chemie), Prof. Dr. Franz Narberhaus (Biologie), Prof. Dr. Nils Pohl (Elektro- und Informationstechnik), Prof. Dr. Tatjana Scheffler (Philologie), Prof. Dr. Gregor Schöner (Informatik), Prof. Dr. Sabine Seehagen (Psychologie), Prof. Dr. Roland Span (Maschinenbau), Prof. Dr. Marc Wichern (Bau- und Umweltingenieurwissenschaft), Prof. Dr. Peter Wick (Evangelische Theologie)

REDAKTIONSANSCHRIFT: Dezernat Hochschulkommunikation, Redaktion Rubin, Ruhr-Universität Bochum, 44780 Bochum, Tel.: 0234/32-25228, rubin@rub.de, news.rub.de/rubin

REDAKTION: Dr. Julia Weiler (jwe, Redaktionsleitung); Meike Drießen (md); Dr. Lisa Bischoff (lb); Raffaela Römer (rr)

FOTOGRAFIE: Damian Gorczany (dg), Schiefersburger Weg 105, 50739 Köln, Tel.: 0176/29706008, damiangorczany@yahoo.de, www.damiangorczany.de; Roberto Schirdewahn (rs), Offerkämpe 5, 48163 Münster, Tel.: 0172/4206216, post@people-fotograf.de, www.wasaufdieaugen.de; Tim Kramer (tk), Agentur für Markenkommunikation, Ruhr-Universität Bochum

COVER: RUB, Tim Kramer

BILDNACHWEISE INHALTSVERZEICHNIS: Teaserfoto für Seite 14: Roberto Schirdewahn; Seite 22, 62: RUB, Tim Kramer

GRAFIK, ILLUSTRATION, LAYOUT UND SATZ:
Agentur für Markenkommunikation, Ruhr-Universität Bochum, www.einrichtungen.rub.de/de/agentur-fuer-markenkommunikation. Die Illustrationen wurden mit Adobe Firefly erzeugt.

DRUCK: LD Medienhaus GmbH & Co. KG, Hansaring 118, 48268 Greven, info@ld-medienhaus.de, www.ld-medienhaus.de

ANZEIGEN: Dr. Julia Weiler, Dezernat Hochschulkommunikation, Redaktion Rubin, Ruhr-Universität Bochum, 44780 Bochum, Tel.: 0234/32-25228, rubin@rub.de

AUFLAGE: 3.900

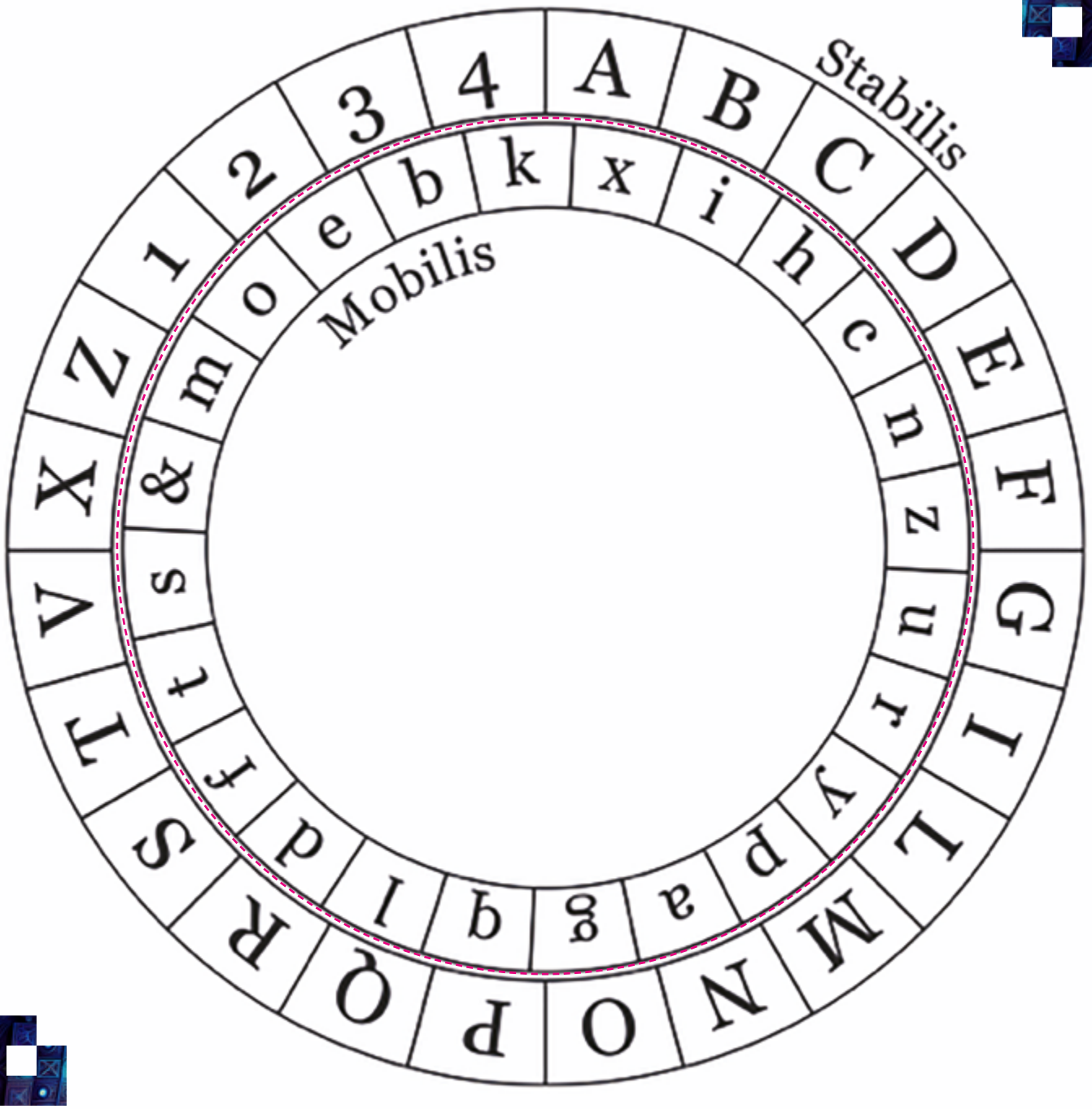
BEZUG: Rubin erscheint zweimal jährlich und ist erhältlich im Dezernat Hochschulkommunikation der Ruhr-Universität Bochum. Das Heft kann kostenlos abonniert werden unter news.rub.de/rubin/abo. Das Abonnement kann per E-Mail an rubin@rub.de gekündigt werden.

ISSN: 0942-6639

Die nächste Ausgabe von RUBIN erscheint am 1. Dezember 2025.

Lösungssatz: Viel Freude beim Lesen von Rubin

CHIFFRIERSCHEIBE



Den inneren Ring der Scheibe ausschneiden und los geht's.