Gegenvorschlag zur Motion des Bitcoin-Verbots zur effizienten Bekämpfung von Cyberkriminalität und Ransomware

TL;DR : Bitcoin zu verbieten ist technisch nicht möglich und wird das Problem der Cyberkriminalität nicht lösen. Daher schlage ich durchsetzbare und gezieltere Massnahmen zur Bekämpfung von Ransomware vor: ein Verbot von Lösegeldzahlungen, Massnahmen zur Unterstützung der Opfer und die Stärkung von präventiven Massnahmen in der Cybersicherheit.

Dieser Vorschlag wurde als Reaktion auf die Motion 21.4068 von Roger Nordmann verfasst.

Die Finanzierungsquellen von Cyberkriminellen zum Versiegen bringen

Meines Erachtens enthält die Motion keine geeigneten Massnahmen zur Sicherstellung der Cybersicherheit in der Schweiz und kann nicht wirksam sein, wenn keine ergänzende Massnahmen erlassen werden.

Zur Verhinderung von Lösegeldzahlungen schlagen Roger Nordmann und die Mitunterzeichnenden der Motion 21.4068 ein Verbot von anonymen Kryptowährungen vor. Das Verbot gilt für den Zahlungsverkehr auf öffentlichen Blockchains, welche das Finanzwesen und Zahlungssystem in den kommenden Jahrzehnten revolutionieren werden. Betroffen sind die Schweizer Bevölkerung, Schweizer Unternehmen und Banken. Diese Massnahme ist unverhältnismässig und ohne Überwachungsstaat technisch nicht durchsetzbar. Auch wird das Verbot die Opfer von Cyberkriminalität nicht daran hindern, das Lösegeld zu bezahlen, sei es in Bitcoin oder auf anderem Wege, zum Beispiel im Ausland.

Ich bin überzeugt, dass wirksame Massnahmen zielgerichtet und unkompliziert sein müssen:

1) Einführung einer Melde- und Anzeigepflicht für jede Cyberattacke, welche in den Zuständigkeitsbereich der Schweiz fällt.

2) Verbot von Lösegeldzahlungen von Opfern von Cyberattacken.

3) Verbot für Versicherungsgesellschaften zur Deckung von Risiken von Lösegeldzahlungen.

Cyberkriminelle bereichern sich nicht an Bitcoin, sondern an den Lösegeldzahlungen ihrer Opfer. Deshalb soll keine ungerechtfertigte Schuldzuweisung an Kryptowährungen gemacht werden.

Unterstützende Massnahmen

Ich bin mir darüber im klaren, dass Sicherheitsmassnahmen, welche die Opfer direkt betreffen, heikel sind. Jedoch hängt die Zahlung von Lösegeld alleine von ihnen ab. Daher muss eine solch schwerwiegende Massnahme direkt unterstützt werden:

1) Psychologische Betreuung und Stressbewältigung in allen Landessprachen um die Opfer bei der Bewältung des Traumas zu unterstützen. (Zum Thema digitale Integrität lade ich Sie dazu ein, das Buch OUR PRECIOUS DIGITAL INTEGRITY zu lesen.)

2) Schaffung einer Stelle für Krisenmanagement für den Umgang mit Cyberkriminellen unter Anwendung bewährter Strategien zur Bekämpfung und Identifikation von Cyberkriminellen. Dabei sollen alle bereits zur Verfügung stehenden Instrumente genutzt werden, namentlich die internationale polizeiliche und justizielle Zusammenarbeit, die Zusammenarbeit mit Banken und Kryptowährungsplattformen, die Nutzung von KYC-Daten, welche bereits heute gesammelt werden und Analysen von on-chain Daten von öffentlichen Blockchains wie Bitcoin.

3) Ein spezialisierter Informatikdienst, welcher Daten sichert und zur Schadensbegrenzung beiträgt.

4) Finanzielle Entschädigung der Opfer zur Bewältigung der Folgen des Datenverlustes und des Kontrollverlustes über die Informatikinfrastruktur, sofern die vom Bund vorgeschriebenen Sicherheitsanforderungen erfüllt wurden.

Diese Angelegenheit betrifft die nationale Sicherheit und sollte folglich in den Zuständigkeitsbereich der Bundespolizei oder des Militärs fallen. Die tatkräftige Unterstützung der Opfer und die Schaffung von Alternativen zur Lösegeldzahlung sind dabei zentral.

Präventive Massnahmen

Am wichtigsten sind präventive Massnahmen zur Verhinderung von Hackerangriffen und zur Verbesserung der nationalen Sicherheit. Solche könnten sein:

1) Erstellung einer ausführlichen Liste bewährter Massnahmen im Bereich Sicherheit und Datenschutz sowie eines Qualitäts- oder Sicherheitssiegels, welches nicht spezialisierten Entscheidungsträgern ermöglicht, Sicherheitsrisiken in ihrer Informatikinfrastruktur abzuschätzen.

2) Bei Bedarf wird den Unternehmen die Infrastruktur aus der öffentlichen Hand zur Verfügung gestellt, welche einem sehr hohen Sicherheitsanspruch gerecht wird.

3) Eine Inspektionsstelle zur Informatiksicherheit welche sicherstellt, dass die kritische Infrastrukturen und Unternehmen, welche einem Gütesiegel unterliegen, den Normen entsprechen.

Das Gütesiegel könnte obligatorisch sein, sobald eine kritische Grösse erreicht ist. Gleichzeitig aber sollte es zwingend mit Unterstützungsmassnahmen wie Entschädigungen oder der Datenwiederherstellung verknüpft sein.

Jene Massnahmen orientieren sich an Grundsätzen, welche bereits in anderen Sektoren gelten, in welchen Sicherheit eine wichtige Rolle spielt, wie zum Beispiel in der Baubranche oder bei der Arbeitssicherheit.

Finanzierung

Die nationale Cybersicherheit ist eine Frage der Sicherheit und Verteidigung. Analog zur Armee und Polizei sollen alle Repressions- und Krisenhilfsmassnahmen aus dem ordentlichen Haushalt vom Bund und den Kantonen finanziert werden.

Zusätzliche Massnahmen könnten von den Begünstigten selbst finanziert werden, beispielsweise in Form einer «Basis»-Versicherung, welche kleinen Akteuren empfohlen wird und ab einer kritischen Grösse oder bei einer nachweislichen strategischen Relevanz obligatorisch ist. Im Bereich der Cybersicherheit könnte diese Versicherung eine ähnliche Rolle wie die SUVA bei der Sicherheit und Unfallverhütung spielen.

Organisiert werden diese Strukturen in privaten, halbstaatlichen oder öffentlichen Strukturen.

Schlussfolgerung

In einem zusammenfassenden Antrag würde mein Vorschlag wie folgt lauten:

> Der Bundesrat wird beauftragt:
>
> 1) zur Einführung einer Meldepflicht aller Cyberattacken, welche in die Zuständigkeit der Schweizerischen Eidgenossenschaft fallen.
>
> 2) Lösegeldzahlungen oder anderen Zuwendungen an Personen, welche im Zusammenhang mit Cyberattacken stehen zu verbieten.
>
> 3) die Risikoabsicherung einer Lösegeldforderung infolge einer Cyberattacke zu verbieten.
>
> 4) spezifische Unterstützungsmassnahmen für die Opfer von Cyberangriffen und das Krisenmanagement festzulegen.
>
> 5) Sicherheitsanforderungen für öffentliche und private Informatikinfrastrukturen festzulegen und die Überwachung der Einhaltung dieser Anforderungen sicherzustellen.
>
> 6) eine gemeinsame finanzielle Beteiligung an der globalen Cybersicherheit der Schweiz zu prüfen.
>
> Mir ist bewusst, dass dieser Vorschlag nicht perfekt ist und vor der Veröffentlichung noch die Maschinerie der Schweizer Institutionen durchlaufen muss. Jedoch bin ich von den folgenden Vorteilen überzeugt:

1) Der Vorschlag bedroht nicht die individuelle Freiheit der Schweizerinnen und Schweizer.

2) Die Hauptprobleme der Piraterie in der Schweiz werden behandelt und nicht nur ein Aspekt davon.

3) Die Verbesserung der Cybersicherheit in unserem Land wird gefördert anstatt Spezialisten zu vergraulen, welche zur Forschung und Entwicklung von «open-source» Protokollen wie Bitcoin beitragen.

4) Der Vorschlag ist ein Kompromiss, da er föderalistisch und individuell ausgestaltet werden kann, durch private Akteure oder staatliche Stellen.

5) Der Vorschlag stützt sich nicht auf die Annahme einer internationalen Zusammenarbeit und Abstimmung.

6) Die Schweizerische Unabhängigkeit in der Digitalisierung wird gestärkt.

Der vorliegende Vorschlag steht den Nationalrätinnen und Nationalräten zur Verfügung, welche einen Gegenvorschlag zum Antrag von Roger Nordmanns Bitcoin-Verbot einreichen möchten.