BESCHLUSS

des Bundesvorstands der FDP, Berlin, 18. März 2024

Cyberangriffe wirksam verhindern und bekämpfen – Eine umfassende Strategie zur Cybersicherheit

Unsere Gesellschaft ist vielfältigen Bedrohungen im digitalen Raum ausgesetzt. Erpresser stehlen oder zerstören Daten. Digitale Bankräuber bedienen sich im Online-Banking ihrer Opfer. International vernetzte Cyberkriminelle handeln mit Passwörtern und ganzen Persönlichkeitsprofilen von Millionen von Menschen auf dem Schwarzmarkt. Cyberkriminalität verzeichnet jährlich zweistellige prozentuale Zuwachsraten, während die Aufklärungsquote auf niedrigem Niveau stagniert.

Neben Kriminellen stellen „staatliche Hacker“ ein zunehmendes Risiko dar. Als die größte Container-Reederei der Welt im Jahr 2017 zum Opfer eines gegen den ukrainischen Staat gerichteten staatlichen Angriffs wurde, konnten dramatische Auswirkungen auf den Welthandel nur knapp abgewendet werden. Aber nicht nur staatliche Institutionen wie Geheimdienste gegnerischer Staaten bedrohen unsere Sicherheit, sondern auch – oftmals hochqualifizierte – Personen, die im Auftrag oder Interesse fremder Staaten agieren. Wir brauchen daher eine Sicherheitsstrategie, die die unterschiedlichen Motivationen von Kriminellen, gegnerischen Staaten und im Interesse von gegnerischen Staaten Handelnden berücksichtigt.

Wir brauchen aber auch einen Mentalitätswandel im Umgang mit den Opfern von Cyberkriminalität. Aus dem Schamgefühl heraus, selbst etwas falsch gemacht zu haben, verzichten die meisten Betrugsopfer darauf, Anzeige zu erstatten. Unternehmen fürchten, es könne ihrem Ruf schaden, wenn sie öffentlich machen, Opfer eines Cyberangriffs geworden zu sein, obwohl sich in der Praxis gezeigt hat, dass Kunden, Lieferanten und Partner mehrheitlich verständnisvoll reagieren. Es muss selbstverständlich sein, dass auch im Bereich der Cyberkriminalität die Schuld nicht bei den Opfern, sondern bei den Tätern liegt. Eine Verringerung der erheblichen Dunkelziffer in diesem Kriminalitätsfeld würde ein zielgerichteteres Vorgehen ermöglichen.

Der Kampf gegen die Bedrohung durch Cyberkriminalität und staatliche Akteure ist für uns Freie Demokraten eine gesamtgesellschaftliche Aufgabe. Darum wollen wir ein gemeinsames europäisches Vorgehen. Darum wollen wir sichere kritische Infrastrukturen. Darum wollen wir effiziente Sicherheitsbehörden und eine auch im digitalen Raum hochkompetente Bundeswehr. Darum wollen wir resiliente Unternehmen und exzellent gebildete Bürgerinnen und Bürger.

Europa

Uns Freien Demokraten ist bewusst, dass Cyberkriminalität nur durch gemeinsame europäische Anstrengungen und internationale Zusammenarbeit wirksam verhindert und bekämpft werden kann. Dabei spielt der von der Europäischen Kommission vorgelegte Cyber Resilience Act (CRA) eine gewichtige Rolle. Die Verordnung muss Verbraucherinnen, Verbraucher und Unternehmen wirksam schützen, ohne Hersteller mehr als nötig mit zusätzlichen Vorschriften zu belasten.

- Wir Freie Demokraten wollen Anreize für Unternehmen schaffen, besonders sichere Produkte und Dienstleistungen anzubieten, und sich dadurch einen Marktvorteil zu sichern. Dazu wollen wir den Cyber Resilience Act so ausgestalten, dass er zum weltweiten Vorbild einer Regulierung in diesem Bereich wird. Dabei muss berücksichtigt werden, inwieweit sich ein Produkt oder eine Dienstleistung im praktischen Einsatz als sicher erweist (zum Beispiel durch konsequentes und schnelles Veröffentlichen und Beheben von bekannt gewordenen Sicherheitslücken). Das Erfüllen von Sicherheitsnormen ist notwendig, aber nicht ausreichend, damit ein Produkt oder eine Dienstleistung ein gutes Sicherheitsniveau erreicht.
- Wir begrüßen den Ansatz des Cyber Resilience Act, Hersteller zu verpflichten, über die Lebensdauer eines Produktes Sicherheits-Updates bereitstellen zu müssen. Der Einsatz eines Produktes, für das der Hersteller keine Updates mehr bereitstellt, muss in kritischen Infrastrukturen ausgeschlossen sein. Hersteller müssen die Möglichkeit erhalten, der Verpflichtung dadurch nachzukommen, dass sie ein Produkt bei den Kundinnen und Kunden durch ein neues, gleich- oder höherwertiges Produkt austauschen. Insbesondere Hersteller von Software, aber auch von bestimmten Hardware-Produkten, können ihre Ressourcen so darauf fokussieren, die aktuelle Produktgeneration möglichst sicher und gut zu machen, statt mehrere alte Produktversionen pflegen zu müssen.
- In nahezu jedem technischen Produkt ist Open-Source-Software enthalten. Sie ist damit ein unverzichtbarer Baustein unserer Infrastruktur. Wir Freie Demokraten wollen sicherstellen, dass die Belange von Entwicklerinnen und Entwicklern, die ihre Leistungen als nicht-kommerzielle Open-Source-Software der Allgemeinheit zur Verfügung stellen, im Cyber Resilience Act angemessen berücksichtigt werden. Wer Open-Source-Software ehrenamtlich entwickelt und kostenlos bereitstellt, kann für diese keine teuren Zertifizierungen durchführen. Die richtigen und wichtigen Anforderungen an Zertifizierungen müssen stattdessen auf die Hersteller zielen, die Open-Source-Software in ihren Produkten verwenden.
- Die Prinzipien „Security by Default“ und „Security by Design“ müssen auch im Cyber Resilience Act umgesetzt werden. Sicherheit beginnt nicht mit der Produktentwicklung, sondern bereits in der Entwurfsphase. Wir Freie Demokraten wollen sicherstellen, dass in allen Prozessen im Produktlebenszyklusmanagement von der Planungsphase bis zur Außerbetriebnahme Sicherheitsaspekte berücksichtigt werden. Elektronische Kommunikation, bei der ein Nachweis der Identifizierung erforderlich ist, soll durch Multi-Faktor-Authentifizierung oder eine ähnlich sichere Technologie geschützt werden.
- Für uns Freie Demokraten hat horizontale (sektorübergreifende) Regulierung Vorrang vor vertikaler (sektorspezifischer) Regulierung. So wird ein Flickenteppich von produktspezifischen Regelungen vermieden.
- Cyberkriminelle machen nicht an Landesgrenzen Halt. Wir Freie Demokraten setzen daher bei der Bekämpfung von Cyberkriminalität auf europäische und internationale Zusammenarbeit. Auf europäischer Ebene wollen wir Europol zu einem echten europäischen Kriminalamt mit eigenen operativen Möglichkeiten ausbauen. Die europäische Cybersicherheitsbehörde

ENISA wollen wir stärken. Aber auch außerhalb Europas wollen wir internationale Kooperationen bei der Bekämpfung von Cyberkriminalität und staatlich organisierten Angriffen mit allen Staaten, die unser Wertesystem teilen, vertiefen.

Kritische Infrastruktur (KRITIS)

Um unsere Freiheit und Sicherheit zu gewährleisten, ist ein funktionierendes staatliches Gemeinwesen und eine zuverlässige Versorgung Voraussetzung. Die dafür notwendigen Einrichtungen und Organisationen werden als kritische Infrastruktur bezeichnet.

Der Ausfall oder Beeinträchtigungen dieser Einrichtungen haben nachhaltig wirkende Versorgungsengpässe, erhebliche Störungen der öffentlichen Sicherheit oder andere dramatische Konsequenzen zur Folge. Die wachsende gegenseitige Abhängigkeit einzelner Organisationen machen diese immer empfindlicher gegen störende Einflüsse und Ereignisse von innen und außen. Zur Sicherstellung der Verfügbarkeit der Leistung ist es entscheidend, sowohl die Betriebssicherheit (Resilienz) als auch die Verteidigungsfähigkeit gegen Angriffe auf die Infrastruktur zu gewährleisten.

Dies betrifft insbesondere die IT, da sie die zentrale Logistik für die Steuerung von Prozessen darstellt, das Internet zur Kommunikation nutzt und damit auch von außen erreichbar ist. Diese Strukturen werden immer häufiger Ziele von Angriffen Cyberkrimineller und ausländischer staatlicher Akteure. Wir Freie Demokraten wollen daher die gesetzlichen Regelungen des IT-Sicherheitsgesetzes entsprechend den Sicherheitsanforderungen der Gesellschaft anpassen.

- Schwellenwerte in der „Verordnung zur Bestimmung Kritischer Infrastrukturen nach dem BSI-Gesetz (BSI-Kritisverordnung – BSI-KritisV)“ müssen so angepasst werden, dass auch die regional wichtigen Versorgungseinrichtungen vom Gesetz erfasst werden. Die Schwellenwerte bestimmen, ab welcher Unternehmensgröße oder Leistung die Einrichtungen von der Verordnung betroffen sind. Im Europäischen Rahmen liefert die EU NIS2-Richtlinie dazu eine verbindliche Vorlage, die bis Herbst 2024 in nationales Gesetz umgewandelt werden muss. EU NIS2 ist die europäische Richtlinie für Cybersecurity bei Betreibern kritischer Infrastrukturen. NIS2 legt Mindeststandards in der EU für die Regulierung kritischer Infrastrukturen (KRITIS) fest und erweitert Betroffenheit und Pflichten deutlich. Spätestens ab Herbst 2024 sollen Unternehmen in 18 Sektoren ab 50 Mitarbeitern und 10 Millionen Euro Umsatz viele Cybersecurity-Pflichten umsetzen. Zahlreiche Versorgungseinrichtungen (Stadtwerke, BHKW etc.) liegen durch ihre nur regionale Bedeutung unter den bestehenden Schwellenwerten und werden daher von der KRITIS-Gesetzgebung nicht erfasst. Auch teilen Versorger ihre Betriebe häufig in rechtlich selbstständige Unternehmen auf, sodass es eine Besitzgesellschaft, eine Betreibergesellschaft und eine Servicegesellschaft gibt. Die gültigen KRITIS-Kriterien treffen dann höchstens auf eine dieser Gesellschaften zu, obwohl alle für den Betrieb erforderlich sind. Die Kritis-Verordnung 2021 (KritisV 1.5), die nach dem IT-Sicherheitsgesetz 2.0 geändert wurde, konnte diese gesellschaftlich relevanten Risikobereiche bisher nicht entschärfen.
- Viele kleine und mittlere Unternehmen (KMU) können die forensische Analyse nach Cyberangriffen nicht eigenständig leisten, da die dazu notwendige Sachkompetenz nicht wirtschaftlich vertretbar aufgebaut werden kann. Wir Freie Demokraten wollen, dass das Bundesamt für Sicherheit in der Informationstechnik (BSI) gemeinsam mit der Cybersicherheitswirtschaft diese Unternehmen unterstützt. Entscheidend dazu sind verbindliche Meldepflichten.

- Kritische demokratische Institutionen (Bundestag, Landtage, Bundesregierung, Landesregierungen, Justiz) müssen die gleichen Anforderungen an Cybersecurity erfüllen, die auch von Unternehmen im Rahmen der EU NIS2-Richtlinie erwartet werden. Die Umsetzung der EU NIS2-Richtlinie in nationale Gesetze muss auch für die demokratischen Institutionen im Rahmen des vergebenen Zeitplans (Herbst 2024) wirksam erfolgen. Maßnahmen müssen dokumentiert und prüfbar sein.
- Der (Aus-)Bau kritischer Infrastruktur darf zukünftig nur von vertrauenswürdigen Unternehmen durchgeführt werden, die nicht mehrheitlich von autokratischen Staaten kontrolliert werden, oder die sonstigen Regelungen oder Mechanismen unterliegen, die fremden Staaten über die verbauten Komponenten Spionage oder Sabotage ermöglichen. Das Risiko, dass in Hard- oder Software versteckte Backdoors eingebaut sind, muss kontrollierbar bleiben. Die Kontrollmöglichkeiten gegenüber autoritär geführten Staaten sind mittel- und langfristig nicht gegeben.

Behörden und Verwaltung

Der deutschen Wirtschaft entsteht durch Cyberkriminalität ein jährlicher Schaden von über 200 Milliarden Euro. Zugleich steigt ständig die Bedrohung, dass Kriminelle oder staatliche Akteure Katastrophenereignisse, wie zum Beispiel einen mehrtägigen landesweiten Stromausfall, auslösen. Wir Freie Demokraten wollen die Sicherheitsbehörden so ausrichten, dass sie effektiv in der Prävention und effizient in der Aufklärung von Cyberkriminalität wirken.

- Wir Freie Demokraten wollen die Rolle des Bundesamtes für Sicherheit in der Informationstechnik (BSI) neu definieren. Wir wollen daher zügig den Ausbau des BSI voranbringen, es aus der Fachaufsicht des Bundesministeriums des Innern und für Heimat (BMI) herauslösen und zu einer unabhängigen Zentralstelle für Cybersicherheit in Deutschland ausbauen. Das erleichtert die Etablierung eines wirksamen Schwachstellenmanagements mit dem Ziel, Sicherheitslücken zu schließen.
- Wir Freie Demokraten fordern, dass staatliches Handeln im Umgang mit Sicherheitslücken in Soft- und Hardware ganz darauf ausgerichtet sein muss, diese so schnell wie möglich zu beheben. Alle Behörden, die Kenntnisse von Sicherheitslücken haben, müssen daher verpflichtet werden, diese an die Hersteller zu melden. Dies schließt aus, dass Sicherheitsbehörden solche Informationen zurückhalten oder sie sich gar am Schwarzmarkthandel mit diesen beteiligen, um sie selbst auszunutzen. Die Schäden, die durch nicht behobene Sicherheitslücken entstehen, die ständig von Cyberkriminellen und staatlichen Akteuren ausgenutzt werden, übersteigen jeden vermeintlichen Nutzen der Quellen-Telekommunikationsüberwachung und Online-Durchsuchung. Wir Freie Demokraten setzen uns in der Bundesregierung dafür ein, dass im Rahmen der geplanten Überwachungsgesamtrechnung die Quellen-Telekommunikationsüberwachung und Online-Durchsuchung endgültig abgeschafft werden.
- Neben dem BSI nehmen auch das Bundesamt für Bevölkerungsschutz und Katastrophenhilfe (BBK) und das Technische Hilfswerk (THW) andere Aufgaben im Bereich der Cybersecurity wahr. Wir Freie Demokraten wollen die Zusammenarbeit dieser Institutionen im Bereich Cybersecurity vertiefen. Das THW hat Erfahrung im Bereitstellen von Notfall-Ausstattungen in andauernden Krisenlagen. Für die öffentliche Hand soll es daher als Cyberhilfe bei schwerwiegenden oder kompletten Ausfällen eine Notfall-IT bereitstellen können, um beispielsweise elementare Verwaltungsdienstleistungen wieder verfügbar zu machen. Dafür soll zu-

künftig den Verwaltungen angeboten werden, Backups in vertrauenswürdigen Rechenzentren oder Clouds von Bundes- oder Landesbehörden vorzunehmen, welche das THW im Rahmen der Notfallhilfe nutzen kann.

- Zu der notwendigen Arbeit von Forscherinnen, Forschern, Expertinnen und Experten, die uns täglich in der Praxis vor Cyber-Bedrohungen schützen, gehört auch die Analyse von, der Umgang mit und der Austausch von Angriffswerkzeugen, die Kriminelle und staatliche Akteure nutzen. Wer uns sicherer macht, darf dafür nicht kriminalisiert werden und braucht Rechtssicherheit. Wir Freie Demokraten wollen daher kurzfristig den „Hackertool-Paragrafen" § 202c StGB so überarbeiten, dass nicht mit Strafverfolgung bedroht werden kann, wer verantwortlich Sicherheitslücken meldet. Mittelfristig setzen wir uns auf europäischer Ebene für eine Neuordnung der Regulierung im Bereich der Computerkriminalität mit dem Ziel ein, dass der „Hackertool-Paragraf" ganz abgeschafft und durch eine Norm ersetzt werden kann, die unter Strafandrohung stellt, Angriffswerkzeuge für Straftaten zu nutzen.
- Zu einer resilienten Infrastruktur gehört, Abhängigkeiten von einzelnen Anbietern zu vermindern (digitale Souveränität). Der öffentlichen Hand mit ihrer erheblichen Marktmacht als Auftraggeber kommt hierbei eine Schlüsselrolle zu. Wir Freie Demokraten wollen, dass Regierung, Behörden und Verwaltung in Ausschreibungen fordern, dass Software unter einer Open-Source-Lizenz bereitzustellen ist. Neben dem Prinzip, von der Gesellschaft bezahlte Leistungen dieser auch zur Verfügung zu stellen („Public Money, Public Code"), ist dies im Hinblick auf Cybersecurity von mehrfachem Nutzen. Durch die höhere Transparenz ist die Sicherheit von Open-Source-Produkten leichter zu evaluieren. Die Wartung kann Dritten übertragen werden, wenn der Hersteller diese nicht mehr ausführen möchte oder kann. Und schließlich wird so auch die Abhängigkeit von Herstellern mit anderen Interessen als unseren reduziert.
- Notfall- und Katastrophenschutzpläne müssen kontinuierlich an die Cyber-Bedrohungslage angepasst werden. Deutschland muss auch auf einen Katastrophenfall, wie zum Beispiel einen mehrtägigen landesweiten Stromausfall durch einen Cyberangriff, vorbereitet sein. Wir Freie Demokraten wollen, dass der Bund und die Länder eine gemeinsame Prioritätenliste erstellen und kontinuierlich anpassen, in welcher Reihenfolge der Betrieb kritischer Infrastrukturen sichergestellt wird, wenn eine Katastrophenlage es nicht ermöglicht, alle kritischen Infrastrukturen aufrechtzuerhalten.
- Die Vermögensabschöpfung ist ein effektiver Bestandteil der Kriminalitätsbekämpfung, zum Beispiel im Bereich der Organisierten Kriminalität, der Korruption und Terrorismusbekämpfung, insbesondere bei grenzüberschreitenden Straftaten. Wir Freie Demokraten wollen, dass auch im Bereich der Cyberkriminalität konsequent von der Möglichkeit Gebrauch gemacht wird, sich aus kriminellen Handlungen ergebende Vermögensvorteile abzuschöpfen und damit auch die Opfer zu entschädigen.

Verteidigung

Staatliche Akteure stellen eine zunehmende Bedrohung unserer Sicherheit dar. So ist dem russischen Angriffskrieg gegen die Ukraine ein jahrelanger digitaler Krieg vorausgegangen. Russische Cyberangriffe richten sich dabei nicht nur gegen die Ukraine selbst, sondern auch gegen ihre Verbündeten und allgemein gegen westliche Staaten. Zur Zeitenwende in der Verteidigungspolitik muss auch gehören, die Bundeswehr zur Verteidigung im Cyberraum zu ertüchtigen.

- Deutschland muss sich nicht nur im Falle eines bewaffneten Konfliktes, sondern auch im Cyberraum wirksam verteidigen können. Wir Freie Demokraten wollen die Bundeswehr konsequent digitalisieren und die digitale Verteidigungsfähigkeit Deutschlands stärken. Zudem muss die Bundeswehr ein attraktiver Arbeitgeber für Cybersecurity-Expertinnen und -Experten – auch für Quereinsteiger – werden. Wie bei der herkömmlichen Landesverteidigung agiert die Bundeswehr auch bei der Cyberverteidigung eingebettet in das Bündnis der NATO. Wir wollen jedoch, dass die Bundeswehr herausgehobene Fähigkeiten im Bereich der Cyberverteidigung erlangt, die sie im Rahmen der Aufgabenteilung bei der Bündnisverteidigung in die NATO einbringen kann.
- Die Bundeswehr bleibt auch im Cyberraum grundsätzlich eine Verteidigungsarmee. Die Cyberverteidigung umfasst alle Maßnahmen, die darauf ausgerichtet sind, tatsächliche oder geplante Cyberangriffe zu verhindern oder ihre Wirkung abzuschwächen. Digitale Vergeltungsschläge (sogenannte „Hackbacks“) lehnen wir Freie Demokraten grundsätzlich ab. Für uns ist selbstverständlich, dass wir auch im Cyberraum Menschenrechte, das humanitäre Völkerrecht und die Werte der westlichen Welt und der NATO achten.
- Die Trennung von Bundeswehr und Polizei sowie die grundgesetzlichen Beschränkungen für die Bundeswehr, im Inneren zu agieren, bleiben auch im Cyberraum erhalten. Die Bundeswehr muss zudem in die Lage versetzt werden, im Verbund mit anderen Bundesbehörden im Cyber- und Informationsraum als Akteur erfolgreich zu bestehen. Die parlamentarische Kontrolle über den Einsatz von Cyber-Fähigkeiten der Bundeswehr muss gewährleistet sein.
- Wir Freie Demokraten setzen uns dafür ein, dass „Cyber Warfare“ (digitale Kriegsführung) international geächtet wird. Dies betrifft insbesondere Cyberangriffe, die sich gezielt gegen die Zivilbevölkerung richten. Täterinnen und Täter müssen wie bei Kriegsverbrechen im herkömmlichen Sinne, zum Beispiel durch den Internationalen Strafgerichtshof, verfolgt werden.

Wirtschaft und Arbeit

Neun von zehn Unternehmen waren bereits von Cyberattacken betroffen. Wir Freie Demokraten unterstützen Unternehmen dabei, sich zu schützen.

- Kleinen und mittelständischen Unternehmen fehlt es häufig am nötigen Fachwissen, um sich adäquat gegen Cyberangriffe abzusichern. Gleichzeitig sind Expertinnen und Experten für dieses Thema am Arbeitsmarkt äußerst schwer zu finden. Wir Freie Demokraten wollen daher, dass das BSI eine Datenbank über verfügbare Cybersecurity-Dienstleister pflegt und diese für KMU zur Verfügung stellt. Außerdem wird eine Cyberfeuerwehr eingerichtet, die bei Angriffen und unmittelbar danach KMU unterstützt, den Betrieb wieder sicherzustellen.
- Wir Freie Demokraten setzen bei der Prävention von Cyberkriminalität auch auf die Zusammenarbeit mit Internet-Providern. Internet-Provider sollten verpflichtet werden, Meldungen von Betroffenen über Angriffe oder Angriffsversuche aus ihren Netzen zu prüfen und ihnen nachzugehen.
- Wie in mittlerweile vielen Bereichen ist Deutschland auch in Bezug auf Cybersecurity-Expertinnen und -Experten in ganz besonderem Maße auf qualifizierte Zuwanderung angewiesen. Dabei ist uns bewusst, dass wir im Wettbewerb mit zahlreichen anderen Ländern um die klügsten Köpfe stehen. Wir wollen, dass Deutschland zu einem attraktiveren Standort für Expertinnen und Experten im Bereich Cybersecurity wird.

Bildung, Forschung und Gesellschaft

Erfolgreiche Cyberangriffe beginnen in der Regel nicht mit dem Ausnutzen technischer, sondern menschlicher Schwächen. Wir Freie Demokraten wollen alle Menschen in die Lage versetzen, sicherheitsbewusst mit digitalen Technologien umzugehen. Denn nur wer Risiken sachlich und korrekt einschätzen kann, kann sein Verhalten daran ausrichten, diese zu minimieren.

- Grundlagenwissen zur Cybersecurity ist Bestandteil der Medienkompetenz. Wir Freie Demokraten wollen, dass im Rahmen des Vermittelns von Medienkompetenz in der Schule auch Aspekte der Cybersecurity berücksichtigt werden. Lehrerinnen und Lehrer wollen wir entsprechend weiterbilden. Neben der reinen Wissensvermittlung müssen Schülerinnen und Schüler auch eine „gesunde Skepsis“ entwickeln. Dies hilft ihnen nicht nur unmittelbar, zum Beispiel Angriffsversuche auf ihre Computerkonten per E-Mail, Messenger oder in den sozialen Medien zu erkennen (Phishing), sondern stärkt sie auch in ihren Fähigkeiten, Angriffe auf unsere Demokratie durch gezielte Fehlinformationen als solche wahrzunehmen.
- Wir Freie Demokraten wollen Cybersecurity als eigenen Lehrinhalt der universitären Ausbildung etablieren. Unser Ziel ist dabei, dass es in Deutschland mindestens eine Exzellenzuniversität im Bereich Cybersecurity mit weltweiter Strahlwirkung gibt.
- Wir Freie Demokraten setzen uns auf nationaler und europäischer Ebene für ein Recht auf Verschlüsselung ein und fordern eine grundsätzliche Verschlüsselung elektronischer Kommunikation. Dabei setzen wir auf starke Ende-zu-Ende-Verschlüsselung ohne Hintertüren und staatliche Schlüsselhinterlegung. Jede Einschränkung des Einsatzes von Kryptografie und jede Verpflichtung zum Offenhalten von Sicherheitslücken lehnen wir ab.
- Entwicklerinnen und Entwickler von Open-Source-Software pflegen diese überwiegend ehrenamtlich. Von wenigen prominenten Open-Source-Projekten abgesehen erhalten sie dafür auch nicht die Wahrnehmung oder Anerkennung, die mit den meisten Formen des ehrenamtlichen Engagements verbunden ist. Nichtsdestotrotz ist auch Open-Source-Software unterhalb der öffentlichen Wahrnehmungsschwelle Bestandteil kritischer Infrastrukturen, sodass Sicherheitslücken in solcher Software verheerende Folgen haben können. Wir Freie Demokraten wollen ein Modell schaffen, das es analog zum ehrenamtlichen Engagement im Technischen Hilfswerk Unternehmen ermöglicht, ihre Mitarbeiterinnen und Mitarbeiter zur Analyse und Behebung von Sicherheitslücken in solcher Open-Source-Software unter Fortzahlung des Arbeitsentgelts freizustellen.