piratenpartei
www.piratenpartei.ch

Piratenpartei Schweiz, 3000 Bern

Sehr geehrter Herr Bundesrat Maurer

Sehr geehrte Damen und Herren

Stellungnahme der Piratenpartei Schweiz zur Meldepflicht von Betreiberinnen kritischer Infrastrukturen für Cyberangriffe (Vernehmlassung 2021/70)

Bezugnehmend auf Ihre Vernehmlassungseröffnung vom 12.01.2022 nehmen wir gerne Stellung und würden es zukünftig sehr begrüssen, wenn wir als politische Partei in ihre Adressatenliste aufgenommen werden.

Im Weiteren finden wir Piraten es sehr bedenklich, dass Sie für die Stellungnahme auf eine proprietäre Software verweisen (Word der Firma Microsoft), wo es doch heute zahlreiche offene und freie Dateiformate gibt. Wir entsprechen ihrem Wunsch mit einer docx-Datei, welche auch in neueren Word Versionen geöffnet werden kann.

Die Piratenpartei Schweiz setzt sich seit Jahren für eine humanistische, liberale und progressive Gesellschaft ein. Dazu gehören die Privatsphäre der Bürger, die Transparenz des Staatswesens, inklusive dem Abbau der Bürokratie, Open Government Data, den Diskurs zwischen Bürgern und Behörden, aber auch die Abwicklung alltäglicher Geschäfte im Rahmen eines E-Governments. Jede neue digitale Schnittstelle und Applikation bedingt aber eine umfassende Risikoanalyse und Folgeabschätzung.

Stellungnahme zur Meldepflicht von Betreiberinnen kritischer Infrastrukturen für Cyberangriffe

Gerne nehmen wir zur wie folgt Stellung: Die Piratenpartei macht sich grundsätzlich für eine Politik stark, welche Probleme ursächlich bekämpft. Deshalb möchten wir vorab darauf hinweisen, dass präventives Schützen statt defensiven Reagierens in Bezug auf Cybersicherheit besser wäre. Wir erachten es darum als wichtig, den Fokus der Cybersicherheit auf Resilienz zu legen. Aus diesem Grund fordern wir frühe Kompetenzförderung in der breiten Masse, sowie eine bessere

Ausbildung von Spezialisten in der IT, der Ausbau der Förderung der Entwicklung von neuen Technologien und die Bereitstellung der dafür notwendigen Ressourcen.

Des Weiteren wäre es zeitgemäss, Mindeststandards für die IT-Sicherheit definieren und diese auch für verbindlich zu erklären. Die in der Nationalen Strategie zum Schutz der Schweiz vor Cyber-Risiken [1] enthaltenen Vorschläge dürfen als gute Ausgangslage hierfür betrachtet werden. Ergänzt werden sollte dies mit einem Gebot zur sicheren Verschlüsselung von jeglicher Kommunikation und Daten.

Gleichzeitig steht im Raum, ob auch eine Haftungsfrage bezüglich IT-Sicherheitsstandards eingeführt werden sollte. Dies könnte durch eine Erweiterung des Produktehaftpflichtgesetzes auf unkörperliche, digitale Produkte ergänzt werden. Insbesondere müssten Hersteller von netzwerkfähigen Geräten verpflichtet werden, Patches oder Updates über einen langfristigen Zeitraum (mindestens 5 Jahre) bereitzustellen.

Darüber hinaus halten wir es für fragwürdig, dass nur Betreiber kritischer Infrastruktur verpflichtet werden sollen Cyberangriffe zu melden. Es werden von "normalen" Unternehmen kaum Fälle gemeldet, dabei könnten durch eine zentrale Meldestelle beispielsweise Ransomware-Angriffe auf viele weitere Unternehmen verhindert werden. Eine Meldepflicht sollte deshalb im Minimum auch auf Organisationen, die im Auftrag vom Staat Aufgaben ausführen, alle Unternehmen, die zu einer ordentlichen Revision, oder gemäss DSG 11a [2] zur Anmeldung einer Datensammlung verpflichtet sind, erweitert werden.

Die Meldemöglichkeit ist dabei so niedrigschwellig wie möglich zu gestalten. Als positiver Anreiz müsste auch ein Angebot analog Art. 74 Abs. 3 seitens des Staates zur Bewältigung eines Vorfalls den meldenden Unternehmen in Aussicht gestellt werden.

Die Piratenpartei vermisst ebenso den Einbezug der zukünftigen Entwicklung in der Digitalisierung. Die aktuelle Vorlage geht mit keinem Wort auf "Künstliche Intelligenz" (oder das was gemeinhin darunter verstanden wird) ein, jedoch wird in absehbarer Zeit immer mehr Entscheidungen von solcher Software getroffen werden und auch zu kritischer Infrastruktur gehören.

Bezüglich der Betreiber kritischer Infrastruktur sollte vor allem auch aus der Vergangenheit gelernt werden. Die Crypto AG hat gezeigt, wie gefährlich Closed Source Systeme für die Sicherheit sind. Die immer noch aktive "Schwesterfirma" der Crypto AG, die Infoguard AG [3], beliefert weiterhin Betreiber kritischer Infrastrukturen in der Schweiz. Dies ist ein enormes, unkalkulierbares Klumpenrisiko. Wir fordern deshalb, dass bei kritischer Infrastruktur in Zukunft nur noch Open Source Software (OSS) verwendet werden darf. Dazu braucht es natürlich eine Übergangsregelung

bis zum EOL (end of life) von bestimmten Systemen. Jedoch *muss* OSS zeitnah ein Grundkriterium für jede Beschaffung in diesem Bereich sein.

Um tatsächlich kritische Infrastruktur auf einem angemessenen hohen Niveau zu betreiben, muss die Schweiz langfristig Ressourcen aufbauen, um Hard- und Software für kritische Infrastruktur selbst zu entwickeln UND zu produzieren. Entsprechende Mittel für Förderung, Ausbildung, Forschung in diesem Bereich sind zur Verfügung zu stellen.

Das NCSC (und nicht der NDB) soll die gemeinsame Cyberlage führen, dokumentieren, kontinuierlich und zeitnah transparent veröffentlichen, Art. 73b Abs 2 ist deshalb entsprechend von "kann" auf "muss" abzuändern. Mit einer solchen Regelung halten wir damit die explizite Weiterleitung an den NDB nach Art. 73c Abs. 1 für obsolet. In jedem Fall muss dieser Passus gestrichen werden, da das Risiko besteht, dass der NDB solche Sicherheitslücken hortet und ausnutzt - entgegen dem Interesse der Bevölkerung.

Darüber hinaus fordert die Piratenpartei einen Kurswechsel, um die Interessenskonflikte zu beheben, die sich aus der aktuellen Cybersicherheitsstruktur der Bundesverwaltung ergeben. Offensiv agierende Akteure wie die Armee, die zivilen Nachrichtendienste und die Justiz verfolgen der Cybersicherheit nicht zuträgliche Interessen. Wir begrüssen, dass in Art. 73b Abs. 3 Sicherheitslücken sofort mit den Betreibern von kritischen Infrastrukturen geteilt werden und fordern eine Ergänzung, dass diese nicht für offensive Cyberspielchen gemäss NDG missbraucht werden dürfen. Ebenso muss Hackern automatisch Straffreiheit im Rahmen von Responsible Disclosure zugesichert werden.

Das UVEK aber auch andere Departemente müssen unserer Meinung nach stärker in die Cybersicherheitsorganisation eingebunden werden. Wir erhoffen uns dadurch eine stärkere Gewichtung der Interessen der Betreiber kritischer Infrastrukturen.

Ferner fordern wir dringlich die Bildung eines finanziell gut ausgestatteten Fonds, aus dem Sicherheitsaudits von weit verbreiteter Software (bspw. Open Source / FOSS) finanziert wird. Es ist in Zukunft mit weiteren Sicherheitsvorfällen in der Grössenordnung wie log4j [4] oder heartbleed [5] zu rechnen und es ist im Interesse Aller, diese von non-profit Organisationen in grösstenteils ehrenamtlicher Arbeit erstellte Software, welche grosse Verbreitung geniesst, auf Herz und Nieren überprüfen zu lassen.

Die in Art. 74b genannten Bereiche sollen auf grosse Medienunternehmen erweitert werden.

Art. 74i ist zu starr formuliert. Für grosse Unternehmen ist eine angedrohte Busse von maximal 100'000 Franken lächerlich. Der Gesetzgeber sollte dies anteilig zum Umsatz des Unternehmens definieren, z.B. auf 4% des Jahresumsatzes.

Abschliessend stellt sich für die Piratenpartei die Frage, ob man im Jahr 2022 immer noch an der mentalen Haltung festgehalten werden soll, dass Informatik, Digitalisierung etc. als reiner Kostenblock angesehen wird, und damit immer noch im EFD anzusiedeln ist. Wir finden es an der Zeit, die Digitalisierung in ihrer Gänze die Wichtigkeit zuzusprechen, die sie auch für unser alltägliches Leben, die Wirtschaft und unsere Zukunft hat. Deshalb fordern wir erneut die Schaffung eines eigenen Departments für Digitalisierung, welches ressourcenmässig den tatsächlichen gesellschaftlichen und volkswirtschaftlichen Wert widerspiegelt.

Schlussbemerkungen

Wir beschränken uns in dieser Stellungnahme auf unsere Kernanliegen. Bei Verzicht unsererseits auf umfassende allgemeine Anmerkungen oder auf Anmerkungen zu einzelnen Regelungen, ist damit keine Zustimmung durch die Piraten zu solchen Regelungen verbunden.

Kontaktdetails für Rückfragen finden Sie in der Begleit-E-Mail.

Quellen:

[1] https://www.ncsc.admin.ch/ncsc/de/home/strategie/strategie-ncss-2018-2022.html

[2] https://www.fedlex.admin.ch/eli/cc/1993/1945_1945_1945/de#art_11_a

[3] https://www.republik.ch/2020/11/11/die-mysterioese-schwesterfirma

[4] https://de.wikipedia.org/wiki/Log4j#Bekanntwerden_einer_Sicherheitslücke_im_Dezember_2021

[5] https://de.wikipedia.org/wiki/Heartbleed

———

Piratenpartei Schweiz, Arbeitsgruppe Vernehmlassungen, 12. April 2022