DIGITALE | GESELLSCHAFT

Digitale Gesellschaft, CH-4000 Basel

Eidgenössischen Finanzdepartements EFD
Generalsekretariat EFD
Bundesgasse 3
3003 Bern

Per E-Mail an: ncsc@gs-efd.admin.ch

14. April 2022

Stellungnahme zur Änderung des Informationssicherheitsgesetzes (ISG) (Vernehmlassung 2021/70)

Sehr geehrte Damen und Herren

Am 17. November 2021 eröffnete der Bundesrat die Vernehmlassung zur Einführung einer Meldepflicht für Cyberangriffe und der damit verbundenen Änderung des Informationssicherheitsgesetzes (ISG). Wir danken Ihnen für die Einladung am Vernehmlassungsverfahren teilzunehmen.

Die Digitale Gesellschaft ist eine gemeinnützige Organisation, die sich für Grund- und Menschenrechte, eine offene Wissenskultur, weitreichende Transparenz sowie Beteiligungsmöglichkeiten an gesellschaftlichen Entscheidungsprozessen einsetzt. Die Tätigkeit orientiert sich an den Bedürfnissen der Bürgerinnen und Konsumenten in der Schweiz und international. Das Ziel ist die Erhaltung und die Förderung einer freien, offenen und nachhaltigen Gesellschaft vor dem Hintergrund der Persönlichkeits- und Menschenrechte.

Gerne nehmen wir zum Entwurf wie folgt Stellung:

Vorbemerkung

Die Digitalisierung und ihr bisher wohl grösstes Werk – das Internet – haben die letzten 20 Jahre geprägt wie keine andere Neuerung. Die wirtschaftlichen und gesellschaftlichen Möglichkeiten, welche der digitale Wandel mit sich bringt, sind enorm und haben schon zu vielen positiven Veränderungen in der Gesellschaft geführt. Im letzten Jahrzehnt hat sich der technologische Wandel aber auch vermehrt von einer dunklen Seite gezeigt: Desinformationskampagnen über soziale Netzwerke, Massenüberwachung und Cyberangriffe sind zu realen Bedrohungen für Wirtschaft und Gesellschaft geworden. Insbesondere Angriffe auf IT-Systeme haben in den letzten Jahren massiv zugenommen. So wurden laut einer Untersuchung der ZHAW ein Drittel aller Schweizer KMU schon einmal Opfer eines Cyberangriffs [1]. Diese Vorfälle kosten die Schweiz jährlich schätzungsweise 9.5 Milliarden CHF [2] und betreffen auch immer öfters Betreiber kritischer Infrastrukturen [3].

Im Lichte dieser Entwicklungen unterstützt die Digitale Gesellschaft den Änderungsvorschlag zum ISG. Zusätzlich sind jedoch weitere Massnahmen dringend nötig.

Meldepflicht für alle

Die Erstellung eines möglichst umfassenden, aktuellen Lagebildes ist ein unabdingbarer Schritt in Richtung höherer IT-Sicherheit in der Schweiz. Aktuell ergibt sich dieses Lagebild aus den freiwilligen Meldungen von Bevölkerung und Wirtschaft an das Nationale Zentrum für Cybersicherheit (NCSC). Im ersten Halbjahr 2021 wurden dem NCSC so rund 10'234 Vorfälle gemeldet. Betrachtet man diese Zahl etwas genauer, wird ersichtlich, dass diese Meldungen grossmehrheitlich aus der Bevölkerung kamen.

So trafen beim NCSC knapp 8'000 Meldungen zu «Fake-Sextortion», Vorschussbetrug, Fake-Support-Anrufen und falschen Paketbenachrichtigungen ein. Angriffstaktiken, welche hingegen auf Unternehmen abzielen, wurden kaum gemeldet. So gingen beim NCSC im ersten Halbjahr 2021 lediglich 94 Meldungen zu Malware ein (insbesondere Verschlüsselungstrojanern; wobei 39 Fälle ein von Privaten eingesetztes Produkt betreffen) [4]. Vergleicht man diese Zahl mit den Schätzungen der Anzahl Schweizer Unternehmen, die bereits Opfer eines Cyberangriffs wurden (siehe oben), kommt man zum Schluss, dass die dem NCSC gemeldeten Angriffe auf Unternehmen die absolute Minderheit darstellen. In anderen Worten: Aus den Meldungen der Schweizer

Wirtschaft an das NCSC lässt sich kein aktuelles Lagebild zur IT-Sicherheit Schweizer Unternehmen ableiten. Es muss also davon ausgegangen werden, dass den politischen und wirtschaftlichen Entscheidungsträgern in der Schweiz aktuell kein hinreichendes Lagebild zur IT-Sicherheit zur Verfügung steht.

Mit Blick auf kritische Infrastrukturen ist dieser Informationsmangel besonders verheerend. Grosse Teile der kritischen Infrastruktur erbringen Dienstleistungen, welche für die Gesellschaft von grundlegender Bedeutung sind. Entsprechend hoch müssen die Ansprüche an ihre Sicherheit sein. Die Digitale Gesellschaft unterstützt deshalb die geplante, im revidierten ISG vorgesehene, verbindliche Meldepflicht von IT-Sicherheitsvorfällen für Betreiber von kritischer Infrastruktur.

Die vorgesehene Meldepflicht ist ein erster, wichtiger Schritt; aus unserer Sicht jedoch nicht hinreichend. Die kritische Infrastruktur stellt nur einen Bruchteil der Schweizer IT-Landschaft dar. Wie oben ausgeführt, betreffen IT-Sicherheitsvorfälle aber Unternehmen in allen Sektoren (und die Gesellschaft insgesamt). Zudem kann davon ausgegangen werden, dass die Bedrohungen, denen Betreiberinnen von kritischen Infrastrukturen ausgesetzt sind, sich nur teilweise mit jenen überschneiden, mit denen der Rest der Wirtschaft zu kämpfen hat. Aus den Daten der neuen Meldepflicht wird sich deshalb nicht ein Lagebild für die ganze Schweiz ableiten lassen. Wir schlagen deshalb vor, dass die Meldepflicht künftig auf alle Bereiche der Schweizer Wirtschaft sowie auf staatliche Behörden und NGO ausgedehnt wird, auch wenn diese keine Betreiber von kritischer Infrastruktur sind, sobald der Vorfall eine entsprechende Relevanz hat.

Wird dem NCSC eine Sicherheitslücke bekannt, die ein Drittprodukt betrifft und bei der nicht davon auszugehen ist, dass sie der Herstellerin bereits bekannt ist, muss die Sicherheitslücke vom NCSC umgehend im Rahmen eines «responsible Disclosure»-Verfahrens der betroffenen Herstellerin gemeldet werden. Zusätzlich sollten dem NCSC Mittel an die Hand gegeben werden, um bei meldenden Organisationen auf die Behebung einer Sicherheitslücke bestehen zu können.

Der Grundsatz, entdeckte (aber noch nicht bekannte) Sicherheitslücken («Zero Day Exploits») im Rahmen eines «responsible-Disclosure»-Verfahrens zu veröffentlichen, sollte neben dem NCSC für alle Bundesstellen gelten, auch für den Nachrichtendienst. Alle Bundesstellen sollen auf den Einsatz von Informatikmitteln verzichten, welche diese Lücken ausnutzen – denn mit solchen «Staatstrojanern» wird das Geschäft mit Sicherheitslücken und damit Unsicherheit vorangetrieben.

Die Digitale Gesellschaft ist sich bewusst, dass eine verbindliche Meldepflicht für die gesamte Wirtschaft nicht unproblematisch ist. Eine Meldepflicht bedeutet technischen und administrativen Aufwand zu einer Zeit, in der eine Organisation einen potenziell existenzgefährdenden Vorfall zu bewältigen hat. Zudem wäre diese Meldepflicht unter Umständen nicht die einzige Meldepflicht, welcher im Falle eines Sicherheitsvorfalls nachgekommen werden müsste. Denkbar – und sogar wahrscheinlich – ist, dass ein Sicherheitsvorfall auch eine Meldepflicht nach dem nDSG nach sich zieht. Zudem wird das betroffene Unternehmen typischerweise auch eine Strafanzeige einreichen wollen. Die Hürden für diese Meldungen sollten deshalb so tief wie möglich gehalten werden. Optimalerweise stünde den Organisationen eine einzige, zentrale Anlaufstelle innerhalb der Bundesverwaltung zur Verfügung, bei der allen Meldepflichten – und potenziell Strafanzeigen – mittels einem einzigen Online-Formular nachgekommen werden kann.

Verbindliche Mindeststandards und Haftung

Neben reaktiven Massnahmen – wie der Meldepflicht – braucht es aber auch proaktive Massnahmen. Wichtig wäre es, verbindliche Mindeststandards zu schaffen, welche überprüfbare «best Practices» definieren. Die im Rahmen der aktuellen Nationalen Strategie zum Schutz der Schweiz vor Cyber-Risiken (NCS) erarbeiteten IKT-Mindeststandards sind ein guter Ansatz, weisen aber folgende drei Mängel auf. Erstens richten sie sich lediglich an Betreiber von kritischer Infrastruktur. Zweitens sind sie für diese nicht verbindlich. Und drittens sind die darin definierten Massnahmen nur sehr schwierig messbar und damit kaum einer Überprüfung zugänglich. Die Digitale Gesellschaft schlägt deshalb die Einführung von verbindlichen Mindeststandards vor, welche sich an den anerkannten Regeln der Technik orientieren und zudem messbare und damit überprüfbare Massnahmen definieren.

Verbindliche Mindeststandards würden es sodann erlauben, eine weitere Herausforderung anzugehen: Die Klärung von Haftungsfragen. Aktuell ist die Frage nach der Haftung für Schäden aus IT-Sicherheitsvorfällen weitgehend ungeklärt. Betroffene, welche durch einen Sicherheitsmangel in der IT einen Schaden erleiden, haben diesen oftmals selbst zu tragen. Grund dafür ist primär die Unklarheit in Bezug auf die Frage, wann IT-Infrastruktur überhaupt einen Sicherheitsmangel aufweist. Verbindliche Mindeststandards würden diese Unsicherheit beseitigen. Die Mindeststandards fungieren in diesem Kontext als ein Mindestmass an «due Diligence», welches eine Betreiberin erreichen muss, um ihre Abnehmer (oder sonstige

mögliche Betroffene) vor Schäden aus Sicherheitsvorfällen zu bewahren. Tut sie das nicht, haftet sie für die Schäden, welche die Betroffenen erleiden.

Zu klären bliebe die Frage nach der Beweislast in diesen Konstellationen. Nach Art. 8 ZGB trägt grundsätzlich jene Partei die Beweislast, welche ein Recht geltend machen will – in Haftungsfragen also grundsätzlich die geschädigte Person. Im Kontext von Schäden, die im Zuge eines IT-Sicherheitsvorfalls entstehen, ist diese Beweislastverteilung aber nicht sinnvoll. Es ist davon auszugehen, dass es dem geschädigten Abnehmer schon allein aufgrund von fehlendem Zugang zur Infrastruktur der Betreiberin in der Regel unmöglich wäre, nachzuweisen, dass die Betreiberin schuldhaft einen Sicherheitsstandard nicht eingehalten hat. Für die Betreiberin hingegen wäre es ein Leichtes, die Einhaltung von Mindestsicherheitsstandards zu protokollieren und somit nachzuweisen. Entsprechend muss im Zusammenhang mit Haftungsfragen betreffend IT-Infrastrukur – in Anlehnung an bereits bestehende Konsumentenschutzgesetze wie das Produktehaftpflichtgesetz (PrHG) – auch über Beweislasterleichterungen oder gar über eine Beweislastumkehr nachgedacht werden.

Ausblick

Die oben aufgeführten Massnahmen stellen einen ersten, entscheidenden Schritt in Richtung mehr IT-Sicherheit dar. Darauf aufbauend sollte aber über weitere Massnahmen nachgedacht werden. Im folgenden werden einige vorgeschlagen.

Die oben diskutierten Mindeststandards bieten zwar eine Hilfestellung zur Klärung von Haftungsfragen bei Schäden aus fehlerhafter IT-Infrastruktur, nicht aber bei Schäden aus fehlerhaften IT-Produkten – also in Konstellationen, in denen eine Herstellerin einem Kunden ein fehlerhaftes IT-Produkt zum eigenen Betrieb übergibt und dem Kunden oder Dritten daraus ein Schaden entsteht. Als Beispiel sind fehlerhafte IoT-Produkte (netzwerkfähige Geräte) oder fehlerhafte Software zu nennen. Das PrHG, welches Haftungsfragen im Kontext von fehlerhaften Produkten klärt, füllt diese Lücke nur teilweise, denn das PrHG ist nur auf bewegliche Sachen anwendbar. In Fällen, in denen das Produkt eine gewisse Körperlichkeit aufweist – wie beispielsweise bei einem Staubsaugerroboter – werden Haftungsfragen also durch das PrHG geklärt. In Fällen, in denen das Produkt jedoch lediglich in digitaler Form vorliegt – wie beispielsweise bei einem Textverarbeitungsprogramm, welches der Kunde direkt von der Website der Herstellerin herunterlädt – fehlt diese Körperlichkeit und das PrHG ist nicht anwendbar. Um diese Lücke zu schliessen, sollte über eine Ausweitung

des Anwendungsbereichs des PrHG auf unkörperliche, digitale Produkte (die gegen ein Entgelt angeboten werden) nachgedacht werden, wie es ein Teil der juristischen Lehre fordert [BSK OR I-Fellmann, Art. 3 PrHG, RZ 10].

Herstellerinnen von netzwerkfähigen Geräten (IoT-Produkte) müssten zudem über einen Zeitraum (abhängig von der durchschnittlichen Nutzungsdauer dieser Geräte) verpflichtet werden, Firmware- und Security-Updates für ihre Geräte allen Nutzern bereitzustellen. Diese «garantierte Nutzungsdauer» entspricht einem Mindeshaltbarkeitsdatum zur sicheren Nutzung und wäre eine Erweiterung der gesetzlichen Gewährleistung.

Wenn Sicherheitsforscher einen Sicherheitsmangel in der Infrastruktur, der Dienstleistung oder dem Produkt eines Unternehmens aufdecken, stellt sich regelmässig die Frage nach der Art und Weise, wie dieser Mangel dem betroffenen Unternehmen gemeldet werden soll. Traditionell waren solche «responsible Disclosures» ein äusserst heikles Unterfangen: Die Sicherheitsforscher mussten trotz ihren guten Absichten damit rechnen, vom Unternehmen, dessen Sicherheitsmangel sie aufgedeckt hatten, verklagt zu werden. In den letzten Jahren hat sich diese Situation etwas entschärft: Das gestiegene Bewusstsein für IT-Sicherheit trägt dazu bei, dass immer mehr Unternehmen dankbar sind für gemeldete Sicherheitsmängel. Einige grössere Unternehmen zahlen im Rahmen von «bug Bounty»-Programmen den Entdeckerinnen von Sicherheitsmängeln gar Belohnungsgelder aus. Insgesamt ist die Situation aber dennoch unbefriedigend. So sorgt insbesondere der Artikel 143bis StGB (sog. «Hackerparagraph»), welcher ein unbefugtes Eindringen in ein Datenverarbeitungssystem oder das Zugänglichmachen von Werkzeugen mit einer Freiheitsstrafe bis zu drei Jahren sanktioniert, weiterhin für erhebliche Rechtsunsicherheit und behindert die Aufdeckung von Sicherheitsmängeln durch Sicherheitsforscher.

Trifft bei einem Unternehmen die Meldung einer Sicherheitslücke ein, so haben insbesondere kleine und mittlere Unternehmen oft nicht die Ressourcen, um umgehend auf die Meldung zu reagieren und die Schwachstelle zu beheben. Das Resultat sind Sicherheitslücken, die zwar erkannt wurden, aber dennoch über lange Zeit offenstehen. Eine zentrale Meldestelle für Sicherheitsmängel könnte Abhilfe schaffen. Eine zentrale Meldestelle innerhalb der Bundesverwaltung – beispielsweise das NCSC – könnte Meldungen von Sicherheitslücken entgegennehmen und alle potenziell betroffenen Unternehmen gleichzeitig informieren. Daraus würden sich

zwei Vorteile ergeben. Einerseits könnte so der Finder bzw. die Finderin der Sicherheitslücke von einer potenziell feindseligen Reaktion des Unternehmens geschützt werden. Andererseits könnte das NCSC auf die Behebung der Sicherheitslücke hinwirken.

Schlussbemerkung

Wir beschränken uns in dieser Stellungnahme auf unsere Kernanliegen. Bei Verzicht auf umfassende allgemeine Anmerkungen oder auf Anmerkungen zu einzelnen Artikeln bedeutet dies keine Zustimmung der Digitalen Gesellschaft.

Freundliche Grüsse

Erik Schönenberger