STABSSTELLE CYBER-SICHERHEIT
FÜRSTENTUM LIECHTENSTEIN

Nationale Strategie zum Schutz vor Cyber-Risiken

Februar 2025

Inhaltsverzeichnis

Zusammenfassung

Liechtenstein verfügt über eine Nationale Strategie zum Schutz vor Cyber-Risiken.[1] Diese breit abgestützte und von einer sachkundigen Begleitgruppe mitentwickelte nationale Strategie wurde von der Regierung am 20. Oktober 2020 verabschiedet, um Liechtenstein vor Cyber-Risiken zu schützen. Die Stabsstelle Cyber-Sicherheit[2] koordiniert die periodische Überprüfung und Aktualisierung dieser Strategie und beschäftigte sich seit dem Frühjahr 2024 mit der ersten vollständigen Überarbeitung derselben.

Das Ergebnis dieser Überprüfung, die vorliegende Nachfolgestrategie, definiert die Vision Liechtensteins im Zusammenhang mit dem Schutz gegen Cyber-Risiken, sie bezeichnet die Anspruchsgruppen und sie legt die Ziele sowie Grundsätze des Handelns fest. Die Strategie berücksichtigt ebenso die jüngsten Entwicklungen im Bereich der Cybersicherheit als auch die aktuellen rechtlichen Verpflichtungen.

Liechtenstein entwickelt und pflegt die Digitalisierung in allen Lebensbereichen zum Wohl der Bevölkerung, der Wirtschaft und der Verwaltung. Liechtenstein schützt sich vor Cyber-Risiken. Dieser Schutz basiert auf Vernetzung, Zusammenarbeit und gegenseitiger Unterstützung aller Beteiligten sowie auf Know-how und eigenverantwortlichem Handeln. Der Schutz stellt die Widerstandsfähigkeit, die Sicherheit, das Vertrauen in die Institutionen und die Attraktivität Liechtensteins auch in Zukunft sicher.[3]

Die Nationale Strategie zum Schutz Liechtensteins vor Cyber-Risiken deckt alle wesentlichen Themen der Cybersicherheit ab. Sie richtet sich an folgende Anspruchsgruppen: die Bevölkerung; die Wirtschaft und den Finanzplatz; die kritischen Infrastrukturen sowie die Staatsorgane.

Mit der Strategie werden insbesondere vier Ziele verfolgt: Sämtliche Anspruchsgruppen (1.) kennen ihre Cyber-Risiken, (2.) sind widerstandsfähig, (3.) sind vernetzt organisiert und (4.) leisten ihren Beitrag.

Die Strategie beinhaltet folgende Grundsätze, nach denen die Anspruchsgruppen handeln, wenn sie sich mit Cyber-Risiken auseinandersetzen:

- informieren, sensibilisieren und ausbilden;
- Ressourcen bündeln und stärken – im Land zusammenarbeiten;
- grenzüberschreitend zusammenarbeiten;
- effizient und wirksam arbeiten;
- messbar und wirkungsvoll umsetzen.

Der in der gegenständlichen Strategie festgehaltene Handlungsbedarf ist in fünf Handlungsfelder gegliedert. In jedem Handlungsfeld (Kapitel 6.1 bis 6.5) sind die Ausgangslage und Absicht sowie die jeweiligen Ziele formuliert, die erreicht werden sollen. Der zur Zielerreichung erforderliche Ressourcenbedarf, inklusive allfälliger politischer und regulatorischer Massnahmen für den Schutz vor Cyber-Risiken, folgt in einem Umsetzungs- und Massnahmenplan.

Die Stabsstelle Cyber-Sicherheit nimmt eine zentrale Rolle in der Umsetzung der gegenständlichen Strategie ein. Sie dient als Anlauf- und Verbindungsstelle für alle Belange im Umgang mit Cyber-Risiken sowie als Drehscheibe für sämtliche Anspruchsgruppen. Sie greift auf ihr nationales und internationales Netzwerk zurück und kann so die Anspruchsgruppen bei den Fragen zu Cyber-Risiken optimal beraten.

Die Umsetzung der Strategie erfolgt kontinuierlich. Die Stabsstelle Cyber-Sicherheit koordiniert in Abstimmung mit der Regierung den Umsetzungs- und Massnahmenplan sowie sämtliche Aktivitäten im

[1] https://www.llv.li//serviceportal2/amtsstellen/stabstelle-cyber-sicherheit/nis-strategie/2020-10-08_schutz-cyber-risiken_strategie_li_v1.1.pdf.
[2] https://scs.llv.li.
[3] Vision, siehe Kapitel 2, S. 5.

Zusammenhang mit der gegenständlichen Strategie und deren Umsetzung. Sie wird unterstützt durch einen Beirat.[4]

Liechtenstein setzt beim Thema Cybersicherheit auf Eigenverantwortung, Vernetzung, Kooperation und Effizienz. Es pflegt eine enge Zusammenarbeit und tauscht sich aus mit den Nachbarländern sowie den zuständigen Stellen im Europäischen Wirtschaftsraum. Liechtenstein vernetzt sich gezielt mit Ländern, die ähnliche Voraussetzungen bezüglich Wirtschaft und Digitalisierung aufweisen und die vor vergleichbaren Herausforderungen stehen. Wo immer möglich werden beim Schutz vor Cyber-Risiken bereits bestehende Organisationen, Strukturen, Abläufe und Synergien genutzt. Entscheide werden so gefällt, dass die verfügbaren und eingesetzten Ressourcen eine möglichst grosse Wirkung entfalten.

Die gegenständliche Strategie gilt ab 1. Februar 2025. Sie wird spätestens nach fünf Jahren auf der Grundlage wesentlicher Leistungsindikatoren bewertet und falls erforderlich aktualisiert.

1. Einleitung

Das Fürstentum Liechtenstein unterstützt, entwickelt und gestaltet die Digitalisierung zum Wohle der Bevölkerung und der Wirtschaft in allen Lebensbereichen. Die Regierung ist sich der damit verbundenen Risiken bewusst und fördert aktiv den Schutz gegen diese Risiken.

Die gegenständliche Nationale Strategie zum Schutz vor Cyber-Risiken definiert die Vision Liechtensteins im Zusammenhang mit dem Schutz gegen Cyber-Risiken, sie bezeichnet die Anspruchsgruppen und sie legt die Ziele sowie Grundsätze des Handelns fest. Sie berücksichtigt ebenso die jüngsten Entwicklungen im Bereich der Cybersicherheit als auch die aktuellen rechtlichen Verpflichtungen.

Was ist unter Cyber-Risiko zu verstehen?

Unter Cyber-Risiken sind Gefährdungen unterschiedlicher Werte zu verstehen, die bei der oder durch die Nutzung von Informations- und Kommunikationstechnologien entstehen können. Sie beeinträchtigen etwa die Verfügbarkeit, die Authentizität, die Integrität oder die Vertraulichkeit von Netz- und Informationssystemen. Somit Gefährdungen, die ein Gerät oder eine Gruppe miteinander verbundener oder zusammenhängender Geräte betreffen, aber auch die elektronischen Kommunikationsnetze sowie digitale Daten, die unter anderem gespeichert, verarbeitet, abgerufen oder übertragen werden.

Cyber-Risiken betreffen zugleich immaterielle Werte, wie beispielsweise die Reputation einer Organisation, den Ruf einer Person oder das öffentliche Vertrauen.

Unter Cybersicherheit werden sämtliche Tätigkeiten verstanden, die notwendig sind, um Netz- und Informationssysteme, die Nutzer solcher Systeme und andere von Cyberbedrohungen betroffene Personen zu schützen.

Merkmale der Strategie

Die Strategie trägt den besonderen Stärken und Merkmalen Liechtensteins Rechnung. Sie baut auf hohe Eigenverantwortung, auf kurze unbürokratische Wege, auf die Vorteile persönlicher Netzwerke und auf starke Kooperationen. Sie soll zu grössenverträglichen Ansätzen und Lösungen für Liechtenstein führen und damit alle Anspruchsgruppen stärken.

[4] Siehe Kapitel 7, S. 13.

Die Strategie ist offen und technikneutral formuliert, um die Ziele, Grundsätze und Handlungsfelder auch auf neue Entwicklungen, Technologien und Fragen im Zusammenhang mit Cyber-Risiken anwenden zu können. So etwa bei der voranschreitenden Digitalisierung der Arbeits- und Verwaltungsprozesse, beim Internet der Dinge, bei intelligenten (Strom-)Netzen (sogenannten Smart Grids) und beim Thema künstlicher Intelligenz. Die Strategie selbst bewertet die Cyber-Risiken nicht, dies wird Teil der Umsetzung der Strategie sein.

Die Strategie bildet für die Regierung die Grundlage, um im Zusammenhang mit den Herausforderungen zum Schutz vor Cyber-Risiken schlüssig und umsichtig entscheiden zu können und sämtliche Anspruchsgruppen entsprechend ihrer Verantwortung einzubinden. Sie ist die Basis dafür, dass Liechtenstein über einen umfassenden und guten Schutz vor Cyber-Risken verfügt.

2. Vision

Liechtenstein entwickelt und pflegt die Digitalisierung in allen Lebensbereichen zum Wohl der Bevölkerung, der Wirtschaft und der Verwaltung. Liechtenstein schützt sich vor Cyber-Risiken. Dieser Schutz basiert auf Vernetzung, Zusammenarbeit und gegenseitiger Unterstützung aller Beteiligten sowie auf Know-how und eigenverantwortlichem Handeln. Der Schutz stellt die Widerstandsfähigkeit, die Sicherheit, das Vertrauen in die Institutionen und die Attraktivität Liechtensteins auch in Zukunft sicher.

3. Anspruchsgruppen

Die gegenständliche Nationale Strategie ist umfassend und deckt die wesentlichen Themen der Cybersicherheit ab. Der Schutz gegen Cyber-Risiken gelingt nur gemeinsam. Alle tragen Mitverantwortung und schützen sich und damit auch Liechtenstein vor den Gefahren, die mit der Digitalisierung verbunden sein können. Die Strategie richtet sich an die folgenden Anspruchsgruppen:

- **die Bevölkerung**
  Einwohnerinnen und Einwohner sowie alle Personen, die in Liechtenstein arbeiten oder sich im Land aufhalten;
- **die Wirtschaft und den Finanzplatz**
  National und international tätige Unternehmen und Organisationen, unabhängig ihrer Grösse (kleine, mittlere als auch Grossunternehmen) und der Branche;
  Bankwesen und Finanzmarktinfrastrukturen, insbesondere als Teil der kritischen Infrastruktur, jedoch nicht ausschliesslich;
- **die kritischen Infrastrukturen**
  Alle wesentlichen und wichtigen Einrichtungen, Bauten und Anlagen, Versorgungssysteme und Dienstleistungen, deren Störungen schwerwiegende Auswirkungen auf die öffentliche Ordnung, die öffentliche Sicherheit, die öffentliche Gesundheit haben oder auch zu einem wesentlichen Systemrisiko für Liechtenstein führen könnten; wie beispielsweise die Energie- und Telekommunikationssysteme oder die Trinkwasserversorgung.
- **die Staatsorgane**
  Fürstenhaus, Landtag, Regierung, Gerichte sowie die Liechtensteinische Landesverwaltung und die Gemeinden.

4. Ziele

Die Anspruchsgruppen kennen ihre Cyber-Risiken

Die Anspruchsgruppen kennen ihre spezifischen Cyber-Risiken. Sie wissen, dass sich diese Risiken schnell verändern und entwickeln können. Sie sind in der Lage, zeitnah und angemessen auf Veränderungen zu reagieren.

Die Anspruchsgruppen sind widerstandsfähig

Die Anspruchsgruppen handeln kompetent und haben die notwendigen Massnahmen zum Schutz vor aktuellen Cyberbedrohungen getroffen (Prävention). Im Ereignisfall reagieren sie rasch und angemessen. Das Schadensausmass eines Sicherheitsvorfalls bleibt verkraftbar und allfällige Schäden kleinstmöglich.

Die Anspruchsgruppen sind vernetzt organisiert

Personen, Unternehmen und Organisationen in- und ausserhalb des Landes, die zum Schutz vor Cyber-Risiken beitragen können, wirken zusammen. Liechtenstein verfügt über ein internationales Netzwerk und nutzt dessen Expertise und Unterstützung. Die Anspruchsgruppen und die für die Cybersicherheit verantwortlichen Akteure sprechen regelmässig über die Bedrohungen und den Schutz vor Cyber-Risiken.

Die Anspruchsgruppen leisten ihren Beitrag

Die Anspruchsgruppen wissen, dass Cyber-Risiken alle betreffen. Sie sind sensibilisiert und setzen angemessene Massnahmen zum Schutz vor Cyber-Risiken um. Die Regierung regt zu eigenverantwortlichem Handeln an. Wo es notwendig ist, werden Vorschriften erlassen.

5. Grundsätze

Die Anspruchsgruppen handeln nach den folgenden Grundsätzen, wenn sie sich mit Fragen des Schutzes vor Cyber-Risiken auseinandersetzen. Die Regierung fördert die Zusammenarbeit und schafft die notwendigen Rahmenbedingungen.

Informieren, sensibilisieren und ausbilden

Die Anspruchsgruppen werden befähigt, eigenverantwortlich und kompetent mit Cyber-Risiken umzugehen. Dies indem sie über aktuelle Entwicklungen und Ereignisse betreffend die Cybersicherheit informiert und sensibilisiert werden. Die öffentliche Hand fördert die Aus- und Weiterbildung zum Umgang mit Cyber-Risiken auf allen Stufen und bei allen Anspruchsgruppen. Sie stärkt so die digitale Kompetenz (Prävention).

Ressourcen bündeln und stärken

Liechtenstein entfaltet seine Stärke beim Schutz vor Cyber-Risiken, indem die öffentliche Hand die Anspruchsgruppen zusammenbringt, vernetzt, deren Bedürfnisse erhebt und deren Stärken nutzt. Sie schafft Rahmenbedingungen, sodass die Anspruchsgruppen vertraulich und offen Informationen austauschen und zusammenarbeiten können. Die öffentliche Hand pflegt den Austausch und die Zusammenarbeit mit wichtigen Partnern und entwickelt gemeinsam mit ihnen Lösungen und Angebote für die Anspruchsgruppen (Public-Private-Partnership).

Grenzüberschreitend zusammenarbeiten

Liechtenstein pflegt eine enge Zusammenarbeit und tauscht sich gezielt mit Staaten und internationalen Organisationen aus, bringt sich aktiv ein, leistet seinen Beitrag für die internationale Gemeinschaft, pflegt und nutzt seine Beziehungen zur Minimierung der Cyber-Risiken (Internationale Vernetzung).

Effizient und wirksam arbeiten

Beim Schutz vor Cyber-Risiken werden – wo möglich – bereits bestehende Organisationen und Abläufe genutzt. Diese sind bei Bedarf gezielt anzupassen. Durch effizientes Handeln entfalten die eingesetzten Ressourcen eine möglichst grosse Wirkung, Entscheide fallen risikobasiert. Liechtenstein nutzt seine kurzen unbürokratischen Wege auch bei der Cybersicherheit.

Messbar und wirkungsvoll umsetzen

Die Umsetzung der Strategie in Handlungsfelder und Massnahmen erfolgt konkret und messbar. Sowohl die Massnahmen wie auch ihre Wirkung werden überprüft und daraus Rückschlüsse für weitere Massnahmen gezogen.

6. Umsetzung der Strategie

Die erste Nationale Strategie (2020 bis 2024) war insbesondere vom Aufbau rechtlicher, organisatorischer und technischer Strukturen im Bereich der Cybersicherheit geprägt und umfasste insgesamt neun Handlungsfelder.[5]

Dem gegenüber fallen in der gegenständlichen Strategie aufgrund der bisher geleisteten Aufbauarbeit bei der Stabsstelle Cyber-Sicherheit und dem am 1. Februar 2025 in Kraft getretenen Cyber-Sicherheitsgesetz (CSG) bestimmte Handlungsfelder weg, werden angepasst oder kommen neu hinzu.

Nach den Konsolidierungen wurden zur Erreichung der strategischen Ziele fünf thematische Handlungsfelder identifiziert, festgelegt und in weiterer Folge näher beschrieben:

- Handlungsfeld 1: Risiken und wichtige Entwicklungen kennen;
- Handlungsfeld 2: Informieren, sensibilisieren und vernetzen;
- Handlungsfeld 3: Wesentliche und wichtige Einrichtungen schützen;
- Handlungsfeld 4: Finanzplatz schützen;
- Handlungsfeld 5: Krisen bewältigen.

Die Beschreibungen (siehe Kapitel 6.1 bis 6.5) enthalten jeweils die Ausgangslage und Absicht sowie den angestrebten Zielzustand. Die zur Erreichung der Ziele erforderlichen Ressourcen und allenfalls notwendigen Politik- und Regulierungsmassnahmen werden in einem zweiten Schritt in einem Umsetzungs- und Massnahmenplan detailliert definiert und sind nicht Gegenstand der gegenständlichen Strategie.

[5] 1. Stabsstelle für Cyber-Sicherheit aufbauen, 2. Risiken kennen, 3. Bevölkerung informieren und sensibilisieren, 4. Kritische Infrastrukturen schützen, 5. Wirtschaft vernetzen, 6. Staatsorgane unterstützen und vernetzen, 7. Empfehlungen entwickeln, 8. Cyber-Defence mit Partnerschaften sicherstellen, 9. Im Ereignisfall koordiniert handeln.

6.1 Risiken und wichtige Entwicklungen kennen

Ausgangslage und Absicht

Zwischen Februar 2023 und Februar 2024 erarbeitete die Stabsstelle Cyber-Sicherheit eine Cyberrisikoanalyse für Liechtenstein. Die Ergebnisse dieser Analyse flossen in Form von zwölf konkreten Cyber-Gefährdungen in die «Gefährdungs- und Risikoanalyse Bevölkerungsschutz 2024»[6] mit ein.

Doch für die einzelnen Anspruchsgruppen ergeben sich unter Umständen abweichende spezifische Cyber-Gefährdungen bzw. Cyberbedrohungen und somit Risiken. Die Kenntnis über die jeweils spezifischen Cyber-Risiken ist jedoch Voraussetzung dafür, wirkungsvolle Massnahmen zu treffen und die verfügbaren Ressourcen zielgerichtet einsetzen zu können. Dabei sind nicht nur die wesentlichen und wichtigen Einrichtungen gefordert.

Liechtenstein wird seinen Beitrag leisten, indem es beabsichtigt:

- eine Übersicht über aktuelle Cyber-Gefährdungen für das Land zu erstellen und periodisch nachzuführen;
- eine laufend aktualisierte Lagebeurteilung – Lagebild über aktuelle Cyberbedrohungen – zu erstellen;
- eine Übersicht über neue technische und regulatorische Entwicklungen zu schaffen, die sich auf die Cybersicherheit in Liechtenstein positiv oder auch negativ auswirken können;
- die Anspruchsgruppen adressatengerecht über die Erkenntnisse zu Cyberbedrohungen, aktuellen Schwachstellen und sicherheitsrelevanten Entwicklungen zu informieren;
- die wesentlichen und wichtigen Einrichtungen, die Finanzunternehmen sowie die Wirtschaft dabei zu unterstützen, selbst Risikoeinschätzungen durchzuführen;
- die wesentlichen und wichtigen Einrichtungen sowie weitere Organisationen und Unternehmen zu motivieren, ihre Erkenntnisse und Erfahrungen untereinander auszutauschen;
- die Forschung und Bildung im Bereich der Cybersicherheit sowie dem Umgang mit Cyberbedrohungen und sicherheitsrelevanten Entwicklungen im IKT-Bereich zu fördern.

Zielzustand

In der kommenden Strategieperiode soll Folgendes erreicht werden:

- Die Übersicht der bevölkerungsschutzrelevanten Cyber-Gefährdungen ist aktuell und öffentlich verfügbar.
- Liechtenstein verfügt über ein aktuelles Lagebild zu den relevanten Cyberbedrohungen.
- Sämtliche Anspruchsgruppen werden regelmässig über aktuelle Cyberbedrohungen und sicherheitsrelevante Entwicklungen informiert.
- Eine Übersicht über aktuelle technische und regulatorische Entwicklungen im Bereich der Cybersicherheit liegt vor und wird adressatengerecht kommuniziert.
- Der regelmässige Austausch (Vernetzung) zwischen den Anspruchsgruppen zu Fragen der aktuellen Cyberbedrohungen und sicherheitsrelevanter Entwicklungen findet statt.
- Der Austausch mit Fachpersonen zu Cyber-Risiken, Cyberbedrohungen und sicherheitsrelevanten Entwicklungen ist etabliert und findet regelmässig statt.
- Der fachliche Austausch und die Zusammenarbeit öffentlicher Stellen mit Forschungs- und Bildungseinrichtungen ist etabliert. Es findet Forschung und Lehre im Zusammenhang mit aktuellen Cyberbedrohungen und Risikomanagementmassnahmen statt.

[6] Gefährdungs- und Risikoanalyse Bevölkerungsschutz, Relevante Gefährdungen und Risikoabschätzung vom April 2024,. https://www.llv.li//serviceportal2/amtsstellen/stabstelle-cyber-sicherheit/nis-strategie/2024-04-30_bericht_update_gefaehrdungsanalyse_fl-kombiniert.pdf.

6.2 Informieren, sensibilisieren und vernetzen

Ausgangslage und Absicht

Mit der zunehmenden Digitalisierung können nicht nur einzelne Unternehmen und Organisationen durch Cyberbedrohungen zu Schaden kommen, sondern die Aufrechterhaltung kritischer, gesellschaftlicher oder wirtschaftlicher Tätigkeiten als Ganzes ist einem wachsenden Cyber-Risiko ausgesetzt.

Gerade die Anspruchsgruppe «Bevölkerung» sowie die kleinen und mittelgrossen Unternehmen der Wirtschaft sind sich oft nicht vollumfänglich bewusst, welchen Bedrohungen sie ausgesetzt sind. Sie verfügen vielfach nur über beschränkte Mittel und das Wissen, um sich gegen Cyberbedrohungen und bestehende Cyber-Risiken angemessen zu schützen. Doch gerade die kleinen und mittelgrossen Unternehmen sind in Liechtenstein ein wichtiger Wirtschaftsfaktor.

Liechtenstein wird seinen Beitrag leisten, indem es beabsichtigt:

- sämtliche Anspruchsgruppen über geeignete Kanäle und Formate, wie z. B. Medienauftritte, Veranstaltungen, Newsletter usw., über die Belange der Cybersicherheit zu informieren. Dabei insbesondere über aktuelle Cyberbedrohungen, Schwachstellen, zweckmässige Schutzmassnahmen und angemessene Verhaltensweisen;
- Rahmenbedingungen zu schaffen, sodass die Anspruchsgruppen sicher Informationen austauschen, zusammenarbeiten und sich gegenseitig unterstützen können;
- bei der Information und Sensibilisierung, wie beispielsweise mit Empfehlungen zur Cyberhygiene und den Einsatz ressourcenschonender Schutzmassnahmen, einen Fokus auf die Bevölkerung sowie die kleinen und mittelgrossen Unternehmen zu legen;
- die Aus- und Weiterbildung zum Umgang mit Cyber-Risiken auf allen Stufen und bei allen Anspruchsgruppen zu fördern;
- die Vernetzung sämtlicher Anspruchsgruppen und dabei insbesondere unter den kleinen und mittelgrossen Unternehmen sowie die öffentlich-private Zusammenarbeit zu fördern;
- Hilfe zur Selbsthilfe anzubieten oder Unterstützung bei der Vorbereitung in Bezug auf die Ereignis- oder die Bewältigung von Sicherheitsvorfällen zu leisten.

Zielzustand

In der kommenden Strategieperiode soll Folgendes erreicht werden:

- Die Anspruchsgruppen erhalten regelmässig, adressatengerecht und niederschwellig aktuelle Informationen zum Thema Cybersicherheit.
- Die Anspruchsgruppen kennen die für sie jeweils zuständigen Ansprechstellen für das Thema Cybersicherheit in Liechtenstein.
- Die nationalen Behörden und öffentlichen Stellen arbeiten im Bereich der Information, Sensibilisierung und Vernetzung zusammen und nutzen Synergien. Wo sinnvoll und möglich werden bestehende Formate genutzt und gegebenenfalls ausgebaut.
- Die Anspruchsgruppen tauschen sich untereinander zum Thema Cyber-Sicherheit und dabei insbesondere über aktuelle Cyberbedrohungen, Schwachstellen, zweckmässige Schutzmassnahmen und angemessene Verhaltensweisen aus.
- Ein regelmässiger (Informations-)Austausch (Vernetzung) sämtlicher Anspruchsgruppen untereinander und gegebenenfalls ebenso über die Anspruchsgruppen hinweg ist etabliert.
- Kleine und mittelgrosse Unternehmen nutzen die vorhandene Unterstützung bei der Umsetzung von Risikomanagementmassnahmen.

6.3 Wesentliche und wichtige Einrichtungen schützen

Ausgangslage und Absicht

Die immer engmaschigere Vernetzung der Gesellschaft, die grossen und grenzübergreifenden Abhängigkeiten im Bereich der Digitalisierung sowie die stetige digitale Weiterentwicklung ebenso im Umfeld der kritischen Infrastruktur bergen – unabhängig der zahlreichen Chancen – auch (Cyber-)Risiken. Cybereignisse sind häufiger, sie sind vielschichtiger und ihr Schadenausmass nimmt zu. Durch die starke Vernetzung und bestehende Abhängigkeiten können schon geringe Störungen und Ausfälle zu erheblichen gesellschaftlichen und wirtschaftlichen Auswirkungen führen.

Die wesentlichen und wichtigen Einrichtungen sind dabei besonders schützenswert. Für viele (kritische) Sektoren ist das reibungslose Funktionieren der Netz- und Informationssysteme unabdingbar. Störungen oder Ausfälle führen zu Sachschäden, finanziellen Verlusten und können das Vertrauen der Nutzerinnen und Nutzer in die Digitalisierung schwächen.

Liechtenstein wird die wesentlichen und wichtigen Einrichtungen unterstützen, indem es beabsichtigt:

- zu proaktivem Handeln zu motivieren;
- den Informationsaustausch zwischen den wesentlichen und wichtigen Einrichtungen untereinander über Cyberbedrohungen und Risikomanagementmassnahmen zu fördern;
- über die freiwillige Meldung von Sicherheitsvorfällen und dessen Mehrwert zu informieren;
- den Informationsaustausch mit weiteren Stellen und Organisationen zu fördern;
- den wesentlichen und wichtigen Einrichtungen Frühwarnungen und Hinweise über aktuelle Cyberbedrohungen zukommen zu lassen;
- über kritische und aktuell in den jeweiligen Sektoren ausgenutzte Schwachstellen zu informieren;
- bei der Überwachung der Netz- und Informationssysteme zu helfen;
- einen gefahrenübergreifenden Ansatz zu verfolgen, der technische, operative und organisatorische Massnahmen beinhaltet und der von physischen Schutzmassnahmen über grundlegende Massnahmen der Cybersicherheit (Cyberhygiene) bis hin zum Einsatz neuer Technologien (künstliche Intelligenz, maschinelles Lernen) reicht;
- Verbindlichkeit durch regelmässige Aufsichtstätigkeit zu schaffen.

Zielzustand

In der kommenden Strategieperiode soll Folgendes erreicht werden:

- Die wesentlichen und wichtigen Einrichtungen werden regelmässig über geeignete Formate und Kanäle über aktuelle Themen der Cybersicherheit informiert, wie beispielsweise auf Veranstaltungen oder im bilateralen Austausch.
- Ein regelmässiger Informationsaustausch unter den wesentlichen und wichtigen Einrichtungen sowie mit weiteren Stellen und Organisationen ist etabliert.
- Sämtliche Anspruchsgruppen, insbesondere die kritischen Infrastrukturen, sind über die Möglichkeit der freiwilligen Meldung von Cybervorfällen oder Bedrohungen informiert und nutzen diese.
- Der Informationsfluss über Schwachstellen, Frühwarnungen und Alarmmeldungen ist etabliert.
- Die wesentlichen und wichtigen Einrichtungen kennen die Cyberbedrohungslage und ihre spezifischen Risiken.
- Die wesentlichen und wichtigen Einrichtungen haben angemessene technische, operative und organisatorische Massnahmen für die Sicherheit der Netz- und Informationssysteme ergriffen.
- Die wesentlichen und wichtigen Einrichtungen erfüllen die Berichtspflicht.
- Die Aufsichtsbehörden nehmen ihre Befugnisse gegenüber den wesentlichen und wichtigen Einrichtungen in angemessener Form wahr.

6.4 Finanzplatz schützen

Ausgangslage und Absicht

Im digitalen Zeitalter ist die Widerstandsfähigkeit der Informations- und Kommunikationstechnologien gegen betriebliche Störungen, d.h. die digitale operationale Resilienz, von Finanzunternehmen für die Gewährleistung der Finanzstabilität und der Marktintegrität sind von entscheidender Bedeutung.

Während bereits heute die allgegenwärtige Nutzung von Netz- und Informationssystemen und der hohe Grad an Digitalisierung und Konnektivität grundlegende Merkmale der Tätigkeiten von Finanzunternehmen darstellen, muss ihre digitale Widerstandsfähigkeit weiter erhöht und in den allgemeinen Betriebsrahmen integriert werden. Die Finanzunternehmen unterliegen daher verschiedenster regulatorischer Anforderungen bezüglich der Sicherheit ihrer Netz- und Informationssysteme.

Liechtenstein unterstützt den Finanzplatz und die Finanzunternehmen in Liechtenstein bei ihren Bestrebungen, die Widerstandsfähigkeit gegenüber Cyber-Gefährdungen zu erhöhen, indem es beabsichtigt:

- Anreize für die Umsetzung von Cybersicherheit und Massnahmen zur Cyberhygiene zu schaffen;
- den regelmässigen und sicheren Informationsaustausch über aktuelle Cyberbedrohungen, Verfahren und Werkzeuge zwischen den Finanzunternehmen untereinander zu fördern;
- den Informationsaustausch mit nationalen und internationalen Stellen und Organisationen, insbesondere mit den kritischen Infrastrukturen, zu fördern;
- die Finanzunternehmen bei der Beschaffung von Informationen zu konkreten den Finanzplatz betreffende Cyberbedrohungen zu unterstützen;
- einen regelmässigen Informationsaustausch über aktuelle Cyberbedrohungen mit den zuständigen (Aufsichts-)Behörde zu etablieren;
- Grundlagen für die behördenübergreifende fachlich Zusammenarbeit zu erarbeiten;
- Verbindlichkeit bei den Finanzunternehmen durch regelmässige Aufsichtstätigkeit zu schaffen.

Zielzustand

In der kommenden Strategieperiode soll Folgendes erreicht werden:

- Die Finanzunternehmen informieren sich über sichere Kanäle gegenseitig über aktuelle Themen der Cybersicherheit, wie beispielsweise über aktuelle Cyberbedrohungen.
- Ein regelmässiger Informationsaustausch unter den Finanzunternehmen ist etabliert.
- Die Finanzunternehmen sind über das Dienstleistungsangebot im Bereich der Cybersicherheit der öffentlichen Stellen, wie beispielsweise den Warn- und Informationsdienst des bei der Stabsstelle Cyber-Sicherheit eingerichteten Computer-Notfallteams (CSIRT.LI), informiert und nutzen dieses.
- Die Finanzunternehmen nutzen die Möglichkeit der freiwilligen Meldung von Sicherheitsvorfällen oder Cyberbedrohungen.
- Die Finanzunternehmen kennen die Cyberbedrohungslage und ihre spezifischen Risiken.
- Die Finanzunternehmen verfügen über einen soliden, umfassenden und gut dokumentierten Risikomanagementrahmen, mit dem die spezifischen Cyber-Risiken entsprechend adressiert werden.
- Die Aufsichtsbehörden nehmen ihre Befugnisse gegenüber den Finanzunternehmen in angemessener Form wahr.
- Ein regelmässiger Informationsaustausch und die Zusammenarbeit zwischen den zuständigen öffentlichen Stellen ist etabliert.

6.5 Krisen bewältigen

Ausgangslage und Absicht

Trotz etabliertem Risikomanagementsystem und korrekt implementierten technischen, operativen und organisatorischen Sicherheitsmassnahmen können Netz- und Informationssysteme von Störungen und Ausfällen betroffen sein. Sei es beispielsweise durch physische Ereignisse, technische Störungen, durch menschliches Versagen oder durch eine von einem Angreifer ausgenutzte noch nicht öffentlich bekannte Schwachstelle in einer verwendeten Hard- oder Softwarekomponente.

Sicherheitsvorfälle können nicht nur den laufenden Betrieb erheblich stören, sondern auch das Vertrauen von Kunden, Partnern und der Öffentlichkeit nachhaltig erschüttern. Die Fähigkeit, (Cyber-)Krisen schnell zu erkennen, zu bewältigen und sich von ihnen zu erholen, ist daher entscheidend für die langfristige Sicherheit und Stabilität von Unternehmen, Organisationen und der Staatsorgane.

Angesichts der bestehenden Cyberbedrohungen, sollten die Anspruchsgruppen nicht nur präventive Sicherheitsmassnahmen ergreifen, sondern einen klaren Plan für den Umgang mit Krisenfällen entwickeln. Die Resilienz gegenüber Cyberbedrohungen erfordert etwa eine schnelle Reaktionsfähigkeit, die kontinuierliche Schulung von Mitarbeitenden und die Implementierung robuster Notfallstrategien.

Liechtenstein unterstützt die Anspruchsgruppen bei der Krisenbewältigung, indem es beabsichtigt:

- eine nationale Krisenorganisation zur Bewältigung von Cybersicherheitsvorfällen grossen Ausmasses und von Krisen aufzubauen und regelmässig zu überprüfen;
- die Anspruchsgruppen, insbesondere die kritischen Infrastrukturen, in die nationale Krisenorganisation mit einzubinden;
- über bewährte Verfahren und Techniken des Krisenmanagements zu informieren;
- die Anspruchsgruppen bei der Ereignisbewältigung durch allgemeine Hilfestellung zu unterstützen;
- im Ereignis- oder Krisenfall die betroffene Einrichtung oder Person durch Bereitstellung von Informationen und allgemeine Analysen zu begleiten;
- an organisationsübergreifenden Übungen teilzunehmen, um den Austausch sowie die Zusammenarbeit im Bereich der Krisenbewältigung bei den Anspruchsgruppen zu fördern.

Zielzustand

In der kommenden Strategieperiode soll Folgendes erreicht werden:

- Die nationale Krisenorganisation zur Bewältigung von Cybersicherheitsvorfällen grossen Ausmasses und von Krisen ist etabliert. Es besteht Kohärenz mit dem geltenden Rahmen für das allgemeine nationale Krisenmanagement.
- Für den Fall einer «Cyber-Krise» sind die Rolle des Landesführungsstabes und die Zusammenarbeit mit den verschiedenen öffentlichen Stellen sowie allenfalls anderen Akteuren festgelegt.
- Die nationale Krisenorganisation auf staatlicher Ebene wird regelmässig mit Übungen getestet.
- In gemeinsamen regelmässigen Übungen testen die Anspruchsgruppen ihre jeweilige Krisenorganisation.
- Die grenzüberschreitende Zusammenarbeit und Unterstützung im Ereignisfall sind definiert und entsprechende Vereinbarungen wurden getroffen.

7. Beirat

Die Stabsstelle Cyber-Sicherheit spielt eine zentrale Rolle bei der Umsetzung der gegenständlichen Strategie. Unterstützt wird sie dabei durch einen sogenannten «Beirat». Als beratendes Gremium bringt der Beirat umfassende Expertise aus verschiedenen Fachbereichen ein und unterstützt die Umsetzung der Strategie mit wertvollen Impulsen. Er unterstützt bei der Identifizierung und Priorisierung von Massnahmen zur Zielerreichung oder auch durch Hinweise auf wichtige Themen und aktuelle Entwicklungen. Er dient als Schnittstelle zwischen Theorie und Praxis.

Der Beirat besteht aus Vertretenden der Anspruchsgruppen, von Akteuren und von Partnern, die insbesondere über Fachkenntnisse in den Bereichen Cybersicherheit, Digitalisierung oder auch Strategieumsetzung verfügen.

Der Beirat ist ein flexibel gestaltetes Gremium, das ausschliesslich beratend tätig ist und ohne feste Regularien oder Geschäftsordnung auskommt. Die Einberufung der Mitglieder in den Beirat erfolgt durch die Stabsstelle Cyber-Sicherheit.

Die Stabsstelle Cyber-Sicherheit koordiniert die regelmässigen Treffen des Beirats und steht den Mitgliedern als Ansprechstelle zur Verfügung.

8. Gültigkeit und Anpassung

Die vorliegende Strategie gilt ab 1. Februar 2025. Sie wird spätestens nach fünf Jahren auf der Grundlage wesentlicher Leistungsindikatoren bewertet und falls erforderlich aktualisiert.