AMT FÜR BEVÖLKERUNGSSCHUTZ
FÜRSTENTUM LIECHTENSTEIN

Nationale Strategie 1.1 für Liechtenstein zum Schutz vor Cyber-Risiken

20. Oktober 2020

Inhaltsverzeichnis

Anhang

Zusammenfassung

Die Regierung hat im August 2020 die erste «Nationale Strategie zum Schutz Liechtensteins vor Cyber-Risiken» verabschiedet. Liechtenstein will die Chancen der Digitalisierung zum Wohl der Bevölkerung, der Wirtschaft und der Verwaltung nutzen und sich vor Cyber-Risiken schützen. Dieser Schutz basiert auf Eigenverantwortung, Know-how, Vernetzung und gegenseitiger Unterstützung aller Beteiligten. Er stellt Sicherheit, Vertrauenswürdigkeit und Attraktivität Liechtensteins auch in Zukunft sicher.

Die Strategie deckt alle wesentlichen Themen der Cybersicherheit ab. Sie richtet sich an vier grosse Zielgruppen in Liechtenstein: die Bevölkerung; die Wirtschaft; die kritischen Infrastrukturen sowie die Staatsorgane.[1]

Mit der Strategie werden die folgenden fünf Ziele verfolgt:

— Alle Zielgruppen kennen ihre Cyber-Risiken

— Infrastrukturen und Organisationen sind widerstandsfähig

— Liechtenstein ist vernetzt organisiert

— Alle Zielgruppen leisten ihren Beitrag

— Liechtenstein spricht über Cyber-Risiken und packt an

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

— Schutz vor Cyber-Risiken bedingt eigenverantwortliches Handeln

— Informieren, sensibilisieren und ausbilden

— Ressourcen im Land bündeln und stärken

— Grenzüberschreitend zusammenarbeiten

— Effizient und wirksam arbeiten

Der in der Strategie festgehaltene Handlungsbedarf wird in neun Handlungsfelder gegliedert. In jedem Handlungsfeld sind Vorgaben formuliert, die in der aktuellen Strategieperiode umgesetzt werden sollen, um den Schutz vor Cyber-Risiken in Liechtenstein zu verbessern.

Eine neu gebildete Stabsstelle für Cyber-Sicherheit bildet das Schlüsselelement der Umsetzung. Die Stabsstelle nimmt für alle Belange im Umgang mit Cyber-Risiken eine Funktion als Anlauf- und Verbindungsstelle sowie als Drehscheibe für die Zielgruppen wahr. Sie greift auf ihr nationales und internationales Netzwerk zurück und kann so ihre Zielgruppen bei den Fragen zu Cyber-Risiken optimal beraten. Die Umsetzung der Strategie wird in Etappen erfolgen, die Stabsstelle wird die Schwerpunkte in den Handlungsfeldern risikobasiert festlegen.

Liechtenstein setzt in der Strategie auf Eigenverantwortung, Vernetzung, Kooperation und Effizienz. Das Land pflegt eine enge Zusammenarbeit mit den Schweizer Behörden und tauscht sich aus mit den Nachbarländern sowie den zuständigen Stellen im Rahmen des EWR-Abkommens. Liechtenstein tauscht sich gezielt mit Ländern aus, 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

1 Institutionen des Landes und der Gemeinden.

Organisationen und Abläufe genutzt. Entscheide werden so gefällt, dass die eingesetzten Ressourcen eine möglichst grosse Wirkung entfalten.

Die Strategie bildet für die Regierung die Basis, um bei den Fragen zum Schutz vor Cyber-Risiken schlüssig und umsichtig zu entscheiden und die Zielgruppen entsprechend ihrer Verantwortung in die Pflicht zu nehmen.

Diese erste Fassung der Strategie ist auf einen Zeithorizont von drei Jahren ab dem Start der Stabsstelle für Cyber-Sicherheit ausgelegt. Um der schnellen Entwicklung der Informations- und Kommunikationstechnologie und der Bedrohungslage Rechnung zu tragen, soll die Strategie spätestens im Frühling 2024 aktualisiert werden.

1. Einleitung

Das Fürstentum Liechtenstein nutzt die Chancen der Digitalisierung und plant, künftig von diesen noch stärker zu profitieren. Die Liechtensteiner Regierung ist sich der damit verbundenen Risiken bewusst und will den Schutz gegen diese Risiken fördern.

Auftrag und Erarbeitung
Um Liechtenstein künftig besser gegen Cyber-Risiken zu schützen und damit auch die Chancen der Digitalisierung weiterhin möglichst in vollem Umfang nutzen zu können, beauftragte die Regierung im Februar 2020 das Amt für Bevölkerungsschutz (ABS), eine «Nationale Strategie für Liechtenstein zum Schutz vor Cyber-Risiken» zu erarbeiten. Die Regierung hat den Auftrag explizit breit formuliert und ein interdisziplinäres Vorgehen empfohlen Da dieses Thema alle Bereiche quer durch die Gesellschaft Liechtensteins betrifft, waren Vertreter der Landesverwaltung, der Gemeinden, der Wirtschaft und der Universität Liechtenstein (vgl. dazu Anhang A2) in die Ausarbeitung der Strategie eingebunden.

Das ABS entwickelte die Strategie mit den aufgeführten Partnern im 1. Semester 2020. Das Projektteam wurde bei der Erarbeitung von einer Kern- und Begleitgruppe unterstützt. Die Strategie zeigt alle bedeutenden Handlungsfelder auf, die risikobasiert zu priorisieren sind und etappiert umgesetzt werden sollen.

Vorarbeiten
Diese Strategie berücksichtigt diverse Vorarbeiten, namentlich die im März 2019 von der Regierung veröffentlichte «Digitale Agenda Liechtenstein», die private Standortinitiative «digital-liechtenstein.li», rechtliche Verpflichtungen wie die «Europäische Richtlinie zur Gewährleistung einer hohen Netzwerk- und Informationssicherheit» (NIS-Richtlinie) der Europäische Union (EU) aus dem Jahr 2016 sowie verschiedene nationale Strategien anderer Länder.

Was ist unter Cyber-Risiken zu verstehen?
Unter Cyber-Risiken sind Gefährdungen unterschiedlichster Werte zu verstehen, die bei der oder durch die Nutzung von Informations- und Kommunikationstechnologien entstehen können. Diese umfassen unter anderem:

— gespeicherte Informationen, die unbefugt manipuliert werden,

— IT-Systeme, die ausfallen oder Fehlfunktionen aufweisen,

— weitere betroffene Anlagen, die von Informations- und Kommunikationstechnologien abhängig sind; etwa im Kleinen eine über das Internet steuerbare Heizung oder im Grossen eine wichtige Versorgungsanlage für eine ganze Region,

— immaterielle Werte, wie die Reputation einer Organisation, den Ruf einer Person bzw. den Schutz der Persönlichkeit, von Urheberrechten, Transparenz und von öffentlichem Vertrauen.

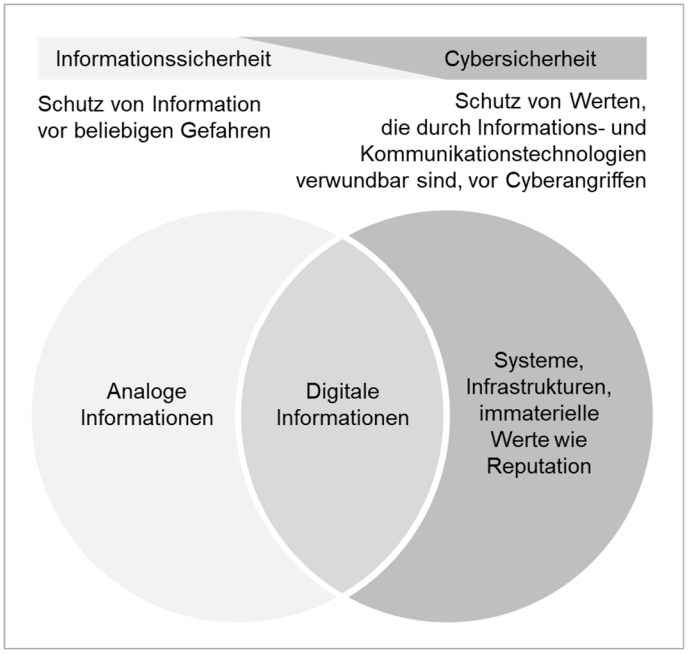

Abbildung 1: Informations- und Cybersicherheit

Vorfälle lassen sich nach verschiedenen Merkmalen kategorisieren: Findet ein Angriff zufällig oder gezielt statt? Durch wen erfolgt der Angriff? Über welches Wissen und über welche Mittel verfügt der Angreifer, und wie geht er vor? Die Bandbreite ist gross und reicht vom «digitalen Schulbubenstreich» über Cyberkriminalität zur finanziellen Bereicherung oder die Beeinflussung demokratischer Prozesse bis hin zum Angriff auf kritische Infrastrukturen durch einen feindlich gesinnten Staat.

Zielgruppen

Die Strategie ist umfassend und deckt alle wesentlichen Themen der Cybersicherheit ab. Weil der Schutz gegen Cyber-Risiken nur gemeinsam gelingt, richtet sie sich deshalb an vier grosse Zielgruppen[2] in Liechtenstein:

— die Bevölkerung: Einwohnerinnen und Einwohner Liechtensteins, aber auch alle anderen Personen, die sich im Land aufhalten;

— die Wirtschaft: kleine und mittlere Unternehmen, Grossunternehmen, aus allen Branchen, national und international tätige;

— die kritischen Infrastrukturen: alle Bauten und Anlagen, Versorgungssysteme und Dienstleistungen, deren Ausfälle gravierende Wirkungen auf das ganze Land haben können. Dazu gehören etwa die Energie- und Telekommunikationssysteme, aber auch die Gemeinschaftswerke, wie z. B. die Wasserversorgung;

— die Staatsorgane: Fürstenhaus, Landtag, Regierung, Landesverwaltung, Gerichte sowie die elf Gemeinden.

Der Schutz vor Cyber-Risiken gelingt nur gemeinsam. Einwohnerinnen und Einwohner, jedes Unternehmen in Wirtschaft und Gewerbe, jede Organisation und jeder Verein, die Staatsorgane, kurz: Alle tragen eine gemeinsame Verantwortung und schützen sich und damit auch Liechtenstein gegen Cyber-Risiken.

2 Die Reihenfolge der Zielgruppen stellt keine Priorisierung und Wertung dar.

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 Zielgruppen stärken.

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 von Arbeits- und Verwaltungsprozessen, beim Internet der Dinge, bei Smart Grids, bei künstlicher Intelligenz und Robotik sowie bei weiteren Themen. Die Strategie selbst bewertet keine Risiken; dies ist Aufgabe im Verlauf der Umsetzung der Strategie.

Die Strategie bildet für die Regierung die Basis, um beim Cyber-Schutz schlüssig und umsichtig zu entscheiden und koordiniert zu handeln. Die Strategie ist die nächsten drei Jahre gültig und spätestens im Frühling 2024 zu aktualisieren. Bei besonderen Entwicklungen oder Ereignissen ist es möglich, die Strategie auch früher anzupassen.

2. Vision

Liechtenstein nutzt die Chancen der Digitalisierung zum Wohl der Bevölkerung, der Wirtschaft und der Verwaltung und schützt sich vor Cyber-Risiken. Dieser Schutz basiert auf Eigenverantwortung, Know-how, Vernetzung und gegenseitiger Unterstützung aller Beteiligten. Er stellt Sicherheit, Vertrauenswürdigkeit und Attraktivität Liechtensteins auch in Zukunft sicher.

3. Ziele

Mit der Strategie zum Schutz vor Cyber-Risiken verfolgt Liechtenstein folgende Ziele:

Alle Zielgruppen kennen ihre Cyber-Risiken
Alle Zielgruppen kennen ihre aktuellen Cyber-Risiken und wissen, dass sich diese Risiken schnell verändern und entwickeln können. Sie sind in der Lage, umgehend auf Veränderungen zu reagieren.

Alle Zielgruppen sind widerstandsfähig
Alle Zielgruppen sind kompetent und haben die notwendigen Massnahmen zum Schutz vor Cyber-Risiken getroffen. Im Ereignisfall reagieren sie schnell und angemessen. Das Schadensausmass eines Cyber-Vorfalls bleibt verkraftbar.

Die Zielgruppen sind vernetzt organisiert
Personen, Organisationen und Ressourcen in und ausserhalb des Landes, die zum Schutz vor Cyber-Risiken beitragen, wirken zusammen. Liechtenstein verfügt über ein internationales Netzwerk, dessen Expertise und Unterstützung es nutzt. Die für den Cyber-Schutz verantwortlichen Akteure sprechen sich ab und treten nach aussen mit einheitlichen Positionen auf.

Alle Zielgruppen leisten ihren Beitrag
Die Zielgruppen wissen, dass Cyber-Risiken alle betreffen. Sie sind sensibilisiert und leisten eigenverantwortlich ihren Beitrag zum Schutz vor Cyber-Risiken.

Die Zielgruppen sprechen über Cyber-Risiken und packen an
Vertreter der Zielgruppen tauschen sich ihren Bedürfnissen entsprechend regelmässig aus über die Bedrohungen und den Schutz vor Cyber-Risiken und schärfen so ihre Aufmerksamkeit. Zusammen identifizieren sie geeignete Massnahmen und setzen sie um.

4. Grundsätze

Die verschiedenen Zielgruppen handeln nach folgenden Grundsätzen, wenn sie sich mit Fragen des Schutzes vor Cyber-Risiken auseinandersetzen. Die Regierung schafft dafür die notwendigen Rahmenbedingungen.

Schutz vor Cyber-Risiken bedingt eigenverantwortliches Handeln
Allen Zielgruppen ist bewusst, dass der Schutz vor Cyber-Risiken jeden einzelnen betrifft und dass alle Beteiligten ihren Beitrag leisten müssen. Alle Zielgruppen handeln mit hoher Eigenverantwortung. Die öffentliche Hand regt die Zielgruppen zu konsequentem Selbstschutz an. Nur wo es notwendig und angezeigt ist, werden Vorschriften erlassen. Die Verantwortlichkeiten der einzelnen Zielgruppen sind transparent und klar ausgewiesen.

Informieren, sensibilisieren und ausbilden
Alle Zielgruppen werden befähigt, souverän mit Cyber-Risiken umzugehen, indem sie regelmässig über die Belange der Cyber-Sicherheit sensibilisiert werden. Die öffentliche Hand informiert, sensibilisiert und vernetzt. Sie regt die Aus- und Weiterbildung zum Umgang mit Cyber-Risiken auf allen Stufen und bei allen Zielgruppen an und stärkt so die digitale Kompetenz.

Ressourcen bündeln und stärken – im Land zusammenarbeiten
Liechtenstein entfaltet seine Stärke beim Schutz vor Cyber-Risiken, indem die öffentliche Hand alle Zielgruppen zusammenbringt, vernetzt und deren Stärken nutzt. Die Bedürfnisse der Zielgruppen sind bekannt und die öffentliche Hand vermittelt gezielt Hilfe und Unterstützung. Sie schafft Bedingungen, dass die Zielgruppen vertraulich und offen Informationen austauschen und zusammenarbeiten. Die öffentliche Hand pflegt den Austausch und die Zusammenarbeit mit grossen Unternehmen aus der Informations- und Telekommunikationsbranche. Gezielt werden Public-Private-Partnerships eingegangen.

Grenzüberschreitend zusammenarbeiten
Liechtenstein pflegt eine enge Zusammenarbeit mit den Schweizer Behörden (NCSC[3], andere) und tauscht sich aus mit den Nachbarländern sowie den zuständigen Stellen im Rahmen des EWR-Abkommens (ENISA[4]). Liechtenstein tauscht sich gezielt mit Ländern aus, die ähnliche Voraussetzungen bezüglich Wirtschaft und Digitalisierung aufweisen und die vor vergleichbaren Herausforderungen stehen. Liechtenstein wirkt mit in internationalen Organisationen (UNO, WTO, OSZE, EWR, EFTA, Europarat) und bringt sich ein bei Entwicklungen im Cyberbereich, die wichtig für das Land werden. Die öffentliche Hand kennt die internationalen Fachgremien und Experten zu Cyber-Risiken, sie pflegen und stärken dieses Netzwerk.

Effizient und wirksam arbeiten
Wo immer möglich sind beim Schutz vor Cyber-Risiken bereits bestehende Organisationen und Abläufe zu nutzen. Diese sind bei Bedarf gezielt anzupassen. Durch effizientes Handeln

3 Nationales Zentrum für Cybersicherheit (→ https://www.melani.admin.ch/melani/de/home/ueber_ncsc/das_ncsc.html)

4 European Union Agency for Cybersecurity / Agentur der Europäischen Union für Cybersicherheit (→ https://www.enisa.europa.eu/)

entfalten die eingesetzten Ressourcen eine möglichst grosse Wirkung, Entscheide fallen risikobasiert. Liechtenstein nutzt seine kurzen unbürokratischen Wege auch beim Cyber-Schutz.

Die «Nationale Strategie für Liechtenstein zum Schutz vor Cyber-Risiken» fördert den Informationsaustausch sowie die Interaktion zwischen den Zielgruppen und den Fachstellen.

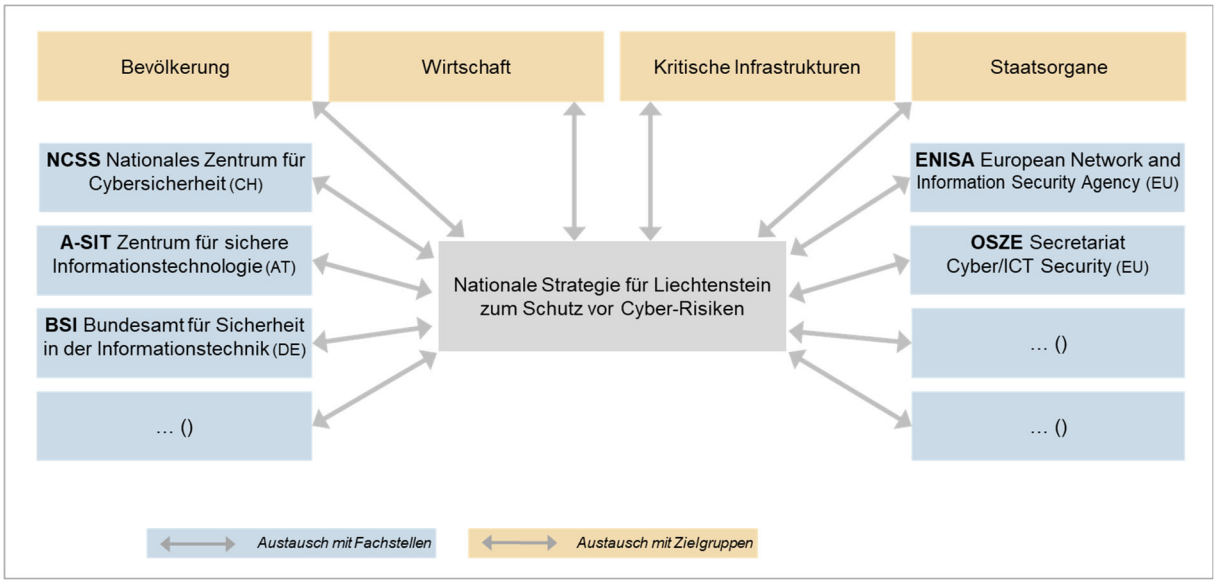

Abbildung 2: Vernetzung aller Akteure (beispielhaft)

5. Handlungsfelder

Um die Vision mit ihren Zielen erreichen zu können, besteht Handlungsbedarf. Dieser lässt sich in neun Handlungsfelder unterteilen. Für jedes Handlungsfeld sind Vorgaben formuliert, die in der kommenden Strategieperiode umzusetzen sind, um den Schutz von Liechtenstein vor Cyber-Risken zu verbessern. Die Reihenfolge der Handlungsfelder stellt keine Priorisierung und Wertung dar. Diese kann erst dann erfolgen, wenn der Zielzustand von Handlungsfeld 1 erreicht ist.

5.1 Stabsstelle für Cyber-Sicherheit aufbauen

Ausgangslage

Der öffentlichen Hand fehlt heute eine Stabsstelle für Cyber-Sicherheit, die für alle Belange im Umgang mit Cyber-Risiken die Funktion als pragmatische, unkomplizierte und dienstleistungsorientierte Anlauf-, Vermittlungs- und Verbindungsstelle (Drehscheibe) für alle Zielgruppen wahrnimmt.

Vorgaben für die Umsetzung

1) Prozesse und Schnittstellen der Stabsstelle definieren.
2) Massnahmenplanung ausarbeiten (was, wer, wie, Kosten, Priorisierung, Termine) und Jahresplanung erstellen.
3) Notwendige wiederkehrende personelle, organisatorische, technische und finanzielle Ressourcen abschätzen.
4) Stabsstelle innerhalb der Landesverwaltung so positionieren, dass eine breite Wirkung, entsteht.
5) Pflichtenheft für die Stabsstelle für Cyber-Sicherheit erstellen mit Aufgaben, Kompetenzen und Verantwortlichkeiten
6) Stellen ausschreiben und besetzen.
7) Aktivitäten im regulären Planungsablauf der Regierung/Landesverwaltung integrieren.
8) Stabsstelle national und international vernetzen.
9) Aufgabenspektrum festlegen.

Zielgruppen

— keine Zielgruppen, nicht relevant für Phase «Aufbau»

Zielzustand (in der ersten Strategieperiode bis Frühjahr 2024 zu erreichen)

— Pflichtenheft ist vorhanden, Prozesse und Schnittstellen sind beschrieben.
— Stabsstelle verfügt über die notwendigen personellen, organisatorischen, technischen und finanziellen Ressourcen und sie ist operativ tätig.
— Stabsstelle kennt die Risiken und hat die Schwerpunkte für ihre Arbeiten in Absprache mit der Regierung festgelegt.
— Stabsstelle ist national und international vernetzt.
— Stabsstelle nimmt ihre Aufgabe als vertrauensvolle Anlauf-, Vermittlungs- und Verbindungsstelle (Drehscheibe) für die Zielgruppen wahr, sie nutzt ihre Kontakte, sie wertet Informationen aus, analysiert, filtert und bereitet auf und bringt Personen, Wissen und Ressourcen zusammen.

— Stabsstelle deckt die Aufgaben aus den Handlungsfeldern 5.2 bis 5.9 ab. Nicht zum Aufgabengebiet gehören technische Analysen oder die Analyse von Einzelfällen. Die Stabsstelle grenzt sich auch von privatwirtschaftlichen Anbietern ab. — Stabsstelle bietet einen unkomplizierten Zugang für alle Zielgruppen. Ihre Funktion reicht von der direkten Beantwortung von Fragen bis hin zur Vermittlung von Fachexperten.
Verantwortlich
1), 2), 3) zuständiges Ministerium 4) Regierung 5), 6) zuständiges Ministerium 7) Stabsstelle 8) alle Stellen gemäss Anhang A2 9) Stabsstelle und zuständiges Ministerium

5.2 Risiken kennen

Ausgangslage

Damit die Stabsstelle für Cyber-Sicherheit angemessen proaktiv und reaktiv mit Cyber-Risiken umgehen und ihre personellen und finanziellen Mittel risikobasiert einsetzen kann, muss sie die aktuellen Cyber-Risiken kennen und vertraut sein mit den aktuellen Entwicklungen in der Informationstechnologie und den diesen verbundenen Risiken.

Vorgaben für die Umsetzung

1) Überblick verschaffen und behalten über aktuelle Cyber-Risiken und Massnahmen durch Austausch mit Zielgruppen und der Fachwelt; grösste Risiken für alle Zielgruppen im Land kennen. Bezug herstellen zu Analysen anderer Länder und zu internationalen Einschätzungen.
2) Prüfen, wie und mit welchen nationalen CERT[5] zusammenzuarbeiten ist (im Vordergrund: GovCERT[6] der Schweiz; Kontakt halten zu FIRST[7] und zu ENISA).
3) Periodisch Gefährdungsanalysen erstellen und überprüfen (generelle und spezifische Analysen). Prüfen, ob periodisch öffentlich über die Lage der Cyber-Sicherheit in Liechtenstein zu informieren ist.
4) Relevante Trends, Themen und Entwicklungen in der Informations- und Kommunikationstechnologie und deren Folgen für zukünftige Cyber-Risiken durch Austausch mit Zielgruppen und der Fachwelt kennen.

Zielgruppen

— Bevölkerung
— Wirtschaft
— Staatsorgane
— Kritische Infrastrukturen

Zielzustand

— Risikolandschaft ist bekannt und nachgeführt.
— Massnahmen bzw. aktueller Handlungsbedarf sind bekannt.
— Risikolandschaft ist analysiert und kommuniziert.

5 Computer Emergency Response Team, Deutsch: Computersicherheits-Ereignis- und Reaktionsteam; eine Gruppe von IT-Sicherheitsfachleuten, die bei der Lösung von konkreten IT-Sicherheitsvorfällen als Koordinator mitwirkt bzw. sich ganz allgemein mit Computersicherheit befasst, Warnungen vor Sicherheitslücken herausgibt und Lösungsansätze anbietet (Quelle: Wikipedia)

6 GovCERT ist das Computer Emergency Response Team der Schweizerischen Bundesverwaltung und das offizielle nationale CERT der Schweiz (→ https://www.govcert.admin.ch/)

7 Forum of Incident Response and Security Teams ist der Dachverband der CERTs und von IT-Sicherheitsfachleuten (→ https://www.first.org/)

— Regierung hat aktuelle Risikolandschaft zur Kenntnis genommen und Aktionsplan verabschiedet.
Verantwortlich
1), 2), 3), 4) Stabsstelle

5.3 Bevölkerung informieren und sensibilisieren

Ausgangslage

Die Bevölkerung ist uneinheitlich und teilweise zu wenig informiert über die Bedeutung von Cyber-Risiken. Die richtigen Verhaltensweisen im privaten und im beruflichen Umfeld sind noch zu wenig bekannt.

Vorgaben für die Umsetzung

1) Ausbildungen zum Thema Cyber-Sicherheit auf allen Stufen anstossen (Pflichtschule, allgemeinbildender und berufsbildender Weg, Fachhochschule, Universität, Erwachsenenbildung); enge Zusammenarbeit mit Bildungssystem anstreben.
2) Freiwillige Weiterbildungen anregen.
3) Spezifischen Fokus auf die Ausbildung von Fachexperten legen.
4) Informationskampagnen durchführen.
5) Bevölkerung über verschiedene Kommunikationskanäle sowohl direkt ansprechen als auch den Austausch suchen über geeignete Organisationen und Gruppierungen, die stellvertretend für die Bevölkerung stehen.
6) Über Ansprechstellen für die Strafverfolgung im Fall von Cyber-Kriminalität informieren.

Zielgruppen

— Bevölkerung

Zielzustand

— Aus- und Weiterbildungsangebot ist vorhanden.
— Bevölkerung nutzt Angebote.
— Regelmässige Informationskampagnen sind durchgeführt.
— Bevölkerung ist auf aktuellem Informationsstand.
— Ansprechstellen für die Strafverfolgung sind bekannt.

Verantwortlich

1), 2), 3) Bildungsinstitute Liechtenstein (Schulamt, etc.)
4), 5), 6) Stabsstelle

5.4 Kritische Infrastrukturen schützen

Ausgangslage

Gemäss dem aktuellen Lagebericht «Sicherheit Schweiz» des Schweizer Nachrichtendienstes des Bundes (NDB) ist mit einer Zunahme von Cyber-Angriffen auf kritische Infrastrukturen zu rechnen. Stehen kritische Infrastrukturen wegen Cyber-Ereignissen nicht oder nur teilweise zur Verfügung, ist das ganze Land unmittelbar betroffen.

Vorgaben für die Umsetzung

1) Die wesentlichen Cyber-Risiken kennen, welche die kritischen Infrastrukturen gefährden.
2) Massnahmen und Handlungsbedarf festlegen.
3) Betreiber der kritischen Infrastrukturen sensibilisieren, ihre Schlüsselaufgaben zu erfüllen, die sich aus der Umsetzung der «Richtlinie zur Gewährleistung einer hohen Netzwerk- und Informationssicherheit» (NIS-Richtlinie) ergeben.
4) Liste kritischer Infrastrukturen mit Fokus «Cyber-Risiken» erstellen und pflegen.

Zielgruppen

— Kritische Infrastrukturen

Zielzustand

— Risiken sind bekannt und Massnahmen identifiziert.
— Betreiber kritischer Infrastrukturen erfüllen NIS-Schlüsselaufgaben.
— Liste der kritischen Infrastrukturen mit Fokus «Cyber-Risiken» ist aktuell.

Verantwortlich

1), 2) Betreiber kritischer Infrastrukturen
3), 4) Stabsstelle; mit landesverwaltungs-interner und -externer Unterstützung

5.5 Wirtschaft vernetzen

Ausgangslage

Liechtenstein weist eine heterogene Wirtschaftsstruktur auf. Je nach Grösse, Branche und IT-Affinität verfügen die verschiedenen Unternehmen über einen unterschiedlichen Reifegrad im Umgang mit Cyber-Risiken.

Vorgaben für die Umsetzung

1) Mit Vertretern aus der Wirtschaft institutionalisierte Zusammenarbeit entwickeln.
2) Als Anlaufstelle und Drehscheibe für die Wirtschaft wirken. Fragen und Anliegen entgegennehmen sowie Kontakte vermitteln.

Zielgruppen

— Wirtschaft

Zielzustand

— Institutionelle Zusammenarbeit im Cyberschutz ist etabliert.
— Anlaufstelle wird durch die Wirtschaft genutzt.
— Informationsstand, Schutz und Widerstandsfähigkeit der Wirtschaft sind verbessert.

Verantwortlich

1), 2) Stabsstelle

5.6 Staatsorgane unterstützen und vernetzen

Ausgangslage

Die Staatsorgane sind unterschiedlich stark sensibilisiert für Cyber-Risiken. Das Fachwissen über Cyber-Risiken ist uneinheitlich und zu wenig vernetzt.

Vorgaben für die Umsetzung

1) Landesverwaltung und Gemeinden bezeichnen Ansprechpersonen zum Thema Cyber-Risiken.
2) In den Staatsorganen periodisch Sensibilisierungskampagnen zum Schutz vor Cyber-Risiken durchführen. Synergien mit dem Amt für Informatik nutzen.
3) Mitarbeitende der Staatsorgane bei Anliegen und Fragen zu Cyber-Risiken unterstützen.
4) Vernetzung unter den bezeichneten Ansprechpersonen fördern. Periodische Treffen zu einem Informations- und Erfahrungsaustausch anregen.

Zielgruppen

— Staatsorgane

Zielzustand

— Ansprechpersonen sind bezeichnet, informiert, sensibilisiert und vernetzt.
— Die Verantwortlichkeit der Stabsstelle innerhalb des Landesverwaltung und das Zusammenspiel mit dem Amt für Informatik sind geklärt.

Verantwortlich

1) Staatsorgane
2) Stabsstelle; zusammen mit dem Amt für Informatik
3), 4) Stabsstelle

5.7 Empfehlungen entwickeln

Ausgangslage

Die Bedrohungslage entwickelt sich laufend weiter. Deshalb werden Massnahmen zum Schutz vor Cyber-Risiken fortwährend weiter- beziehungsweise neu entwickelt; es entstehen regulatorische, organisatorische und technische Vorgaben, Standards und Empfehlungen. Hier gilt es, den Überblick zu halten und zu erkennen, welche Entwicklungen und Themen für Liechtenstein wesentlich sind.

Vorgaben für die Umsetzung

1) Regulatorische und weitere Entwicklungen in anderen Ländern und in internationalen Organisationen kennen und Folgen für Liechtenstein abschätzen.
2) Handlungsbedarf ableiten: Welche Regulierungsvorgaben sind bei Cyber-Risiken einzuhalten? Welche Standards können angewendet werden?
3) Bei Bedarf Empfehlungen oder Vorgaben aus anderen Ländern und internationalen Organisationen für ausgewählte Themen oder für ausgewählte Beteiligte in Liechtenstein adaptieren.
4) Betroffene Zielgruppen über Empfehlungen informieren.

Zielgruppen

— Bevölkerung
— Wirtschaft
— Staatsorgane
— Kritische Infrastrukturen

Zielzustand

— Entwicklungen bei Vorgaben, Standards und Empfehlungen zu Massnahmen sind bekannt.
— Bedeutung für Liechtenstein und seine Zielgruppen sowie Handlungsbedarf sind erkannt.

Verantwortlich

1), 2), 3), 4) Stabsstelle; mit landesverwaltungs-interner und -externer Unterstützung

5.8 Cyber-Defence mit Partnerschaften sicherstellen

Ausgangslage

Unter Cyber-Defence ist die (oft militärisch geprägte) Verteidigung von Computernetzwerken, insbesondere der Schutz kritischer Infrastrukturen und die Informationssicherung für wichtige Organisationen und Regierungseinrichtungen zu verstehen. Für Liechtenstein sind diese Bedrohungen ebenso real wie für seine Nachbarn; ein effektiver Schutz vor möglichen gezielten Cyber-Angriffen ist daher angezeigt. Liechtensteins Möglichkeiten zur Verteidigung sind aufgrund fehlender eigener Streitkräfte aber deutlich eingeschränkt.

Vorgaben für die Umsetzung

1) Möglichkeiten und Grenzen der Cyber-Defence Liechtensteins in einem Konzept aufzeigen.
2) Mit geeigneten Partnern eine Zusammenarbeit bzw. eine Unterstützung vereinbaren, um den Staat vor Angriffen zu schützen und um spezifische Angriffe abzuwehren.

Zielgruppen

— Staatsorgane

— Kritische Infrastrukturen

Zielzustand

— Konzept zum Umgang mit Risiken im Rahmen der Cyber-Defence ist erstellt.

— Vereinbarungen mit Partnern zur Cyber-Defence sind getroffen.

Verantwortlich

1) Prüfen und vorbereiten durch Stabsstelle;
   Entscheid durch zuständiges Ministerium und durch Regierung
2) Stabsstelle; mit landesverwaltungs-interner und -externer Unterstützung, Betreiber kritischer Infrastrukturen

5.9 Im Ereignisfall koordiniert handeln

Ausgangslage

Es ist unklar, wie im Fall eines schweren Cyber-Angriffs das vorhandene Know-how rasch in die zuständigen Krisenorganisationen gelangt.

Vorgaben für die Umsetzung

1) Es ist eine Krisenorganisation für die Ereignisbewältigung bei schweren Cyber-Angriffen zu definieren. Dabei sind Aufgaben, Kompetenzen und Verantwortlichkeiten eines möglichen Cyber-Krisenstabs festzulegen.
2) Im Ereignisfall stellt die Stabsstelle für Cyber-Sicherheit die Verbindung zu Vertragspartnern (gem. 5.8) und zu Experten zugunsten dieser Krisenorganisationen sicher.

Zielgruppen

— keine Zielgruppen, nicht relevant für Phase «Aufbau Krisenorganisation»

Zielzustand

— Krisenorganisation und Verantwortlichkeiten im Ereignisfall sind festgelegt und bekannt.

— Rolle Landesführungsstab und Zusammenarbeit mit der Stabsstelle ist geklärt.

Verantwortlich

1) Landesführungsstab, Mitwirkung Stabsstelle;
   Entscheid durch zuständiges Ministerium und Regierung
2) Stabsstelle

6. Umsetzung der Strategie

Die «Nationale Strategie 1.0. für Liechtenstein zum Schutz vor Cyber-Risiken» trat durch den Beschluss der Liechtensteinischen Regierung im **August 2020** in Kraft und die Regierung sprach die erforderlichen Ressourcen für die Stabsstelle (Personalstellen, finanzielle und andere Mittel). Ziel ist es, die Stabsstelle bis Ende 1. Semester 2021 aufzubauen und personell zu besetzen, damit sie anschliessend ihre Arbeit aufnehmen kann.

Die Strategie führt alle wesentlichen Themen zum Schutz vor Cyber-Risiken auf, und die Handlungsfelder 5.2. bis 5.9 beinhalten eine Vielzahl von noch zu konkretisierenden Massnahmen. Die Realisierung der Massnahmen ist etappiert anzugehen. Die Stabsstelle führt dazu eine Risikoanalyse durch und entscheidet in Abstimmung mit dem Ministerium und der Regierung über die Anpassung und Priorisierung der vorgesehenen Massnahmen.

7. Gültigkeit und Anpassung

Die «Nationale Strategie 1.0 für Liechtenstein zum Schutz vor Cyber-Risiken» ist auf einen Zeithorizont von gut drei Jahren ab dem Start der Stabsstelle für Cyber-Sicherheit ausgelegt. Sie ist spätestens im Frühling 2024 zu aktualisieren.

Verantwortlich für die Aktualisierung ist die Stabsstelle für Cyber-Sicherheit. Sie bindet dazu in geeigneter Form Vertreter aller Zielgruppen ein. Bei besonderen Entwicklungen oder Ereignissen ist es möglich die Strategie früher anzupassen. Der Anstoss dazu gibt die Stabsstelle.

A1 Grundlagen, Vorarbeiten, Gesetze, Verträge, internationale Vereinbarungen

Im Folgenden sind die wichtigsten Grundlagen aufgeführt, die bei der Erarbeitung der Strategie herangezogen worden sind. Die Liste erhebt keinen Anspruch auf Vollständigkeit.

Liechtenstein allgemein

— Projektauftrag ‘Nationale Strategie für Liechtenstein zum Schutz vor Cyber-Risiken‘, Regierung des Fürstentums Liechtenstein, 1. Februar 2020

— Bericht zur Beurteilung der Geldwäscherei-Risiken des Bereichs „Virtual Asset Service Providers“ (VASPs) im Fürstentum Liechtenstein, Financial Intelligence Unit, Januar 2020

— Zwischenbericht der Arbeitsgruppe „NIS“ an die Regierung betreffend das Vorgehen zur Umsetzung der Richtlinie (EU) 2016/1148 über Massnahmen zur Gewährleistung eines hohen gemeinsamen Schutzniveaus von Netz- und Informationssystemen in der Union (NIS-Richtlinie), 27. September 2019

— Abgrenzung Informationssicherheit und Cyber-Sicherheit, Amt für Informatik Liechtenstein, 8. Juni 2019

— Digitale Roadmap, Initiative digital-liechtenstein.li, Mai 2019

— Kriminalität im Internet, Interview mit Kripochef Andreas Schädler, Volksblatt, 8. Januar 2018

— Digitale Agenda Liechtenstein, März 2019, Liechtensteiner Regierung

— Studie «Cyber-Sicherheit in Liechtenstein: Risiken, aktuelle Praxis und Handlungsbedarf» der Initiative digital-liechtenstein.li und der Universität Liechtenstein, Juni 2020

Liechtenstein FMA

— Finanzmarktaufsicht (FMA): FMA-Mitteilung 2018/3 – Umgang mit Cyber-Risiken, Erlass: 25.09.2018, letzte Änderung 24. Februar 2020

— Finanzmarktaufsicht (FMA): FMA-Merkblatt 2019/1 – Orientierungshilfe Cyber-Security, 20. Februar 2019

— Finanzmarktaufsicht (FMA): Selbstbeurteilung Cyberrisiken, Excel-Tool, 20.09.2018

Liechtenstein Gefährdungsanalysen, Kritische Infrastrukturen

— Stromversorgung Liechtensteins in ausserordentlichen Lagen, 2017 bis 2019, Amt für Bevölkerungsschutz Liechtenstein Liechtensteinische Kraftwerke

— Beurteilung kritischer Infrastrukturen in Liechtenstein, 2015 bis 2017, Ministerium für Inneres, Bildung und Umwelt

— Gefährdungsanalyse Liechtenstein; Bericht zur Phase I: Situationsanalyse, Gefährdungsauswahl und Risikoabschätzung; 5. November 2012, Amt für Bevölkerungsschutz Fürstentum Liechtenstein

Europa

— Cybersecurity Strategy 2019-2022, Republic of Estonia, 13. Mai 2019

— NCSS Good Practice Guide, Designing and Implementing National Cyber Security Strategies, European Union Agency For Network And Information Security, November 2016

— Europäische Richtlinie zur Gewährleistung einer hohen Netzwerk- und Informationssicherheit» (NIS-Richtlinie) der Europäische Union (EU), 6. Juli 2016

— Europarat, Übereinkommen über die Computerkriminalität (Convention on Cybercrime), Budapest, in Kraft seit 1. Juli 2004 (Ratifikation durch Liechtenstein am 27. Januar 2016)

Schweiz

— Beurteilung der Bedrohungslage, Bericht des Bundesrates an die eidgenössischen Räte und die Öffentlichkeit, 29. April 2020

— Nationale Strategie zum Schutz der Schweiz vor Cyber-Risiken (NCS) 2018–2022, Informatiksteuerungsorgan des Bundes ISB, 2018

A2 Beteiligte

Projektaufsicht / Auftraggeber
— Emanuel Banzer, Amt für Bevölkerungsschutz, Amtsleiter

Projektleiter ABS
— Markus Schlegel, Amt für Bevölkerungsschutz

Projektteam
— Markus Schlegel, Amt für Bevölkerungsschutz, Projektleitung

— Christof Egli, EBP Schweiz AG, Projektbeauftragter

— Dr. Tillmann Schulze, EBP Schweiz AG, Projektbeauftragter

— Pierina Da Costa, EBP Schweiz AG, Projektbeauftragte

Kernteam
— Markus Schlegel, Amt für Bevölkerungsschutz, Leitung Kernteam

— Patrik Thoma; Amt für Informatik, Information Security Manager

— Dr. Rainer Schnepfleitner, Amt für Kommunikation, Amtsleiter

— Lothar Ritter, Vorsitzender des Boards der Standortinitiative digital-liechtenstein.li

— Christof Egli, EBP Schweiz AG, Projektbeauftragter

— Dr. Tillmann Schulze, EBP Schweiz AG, Projektbeauftragter

— Pierina Da Costa, EBP Schweiz AG, Projektbeauftragte

Begleitgruppe
— Emanuel Banzer, Amt für Bevölkerungsschutz, Amtsleiter, Vorsitz Begleitgruppe

— Roland Bon, Landespolizei

— Dr. Martin Frick, Amt für Auswärtige Angelegenheiten, Amtsleiter

— Dr. Katja Gey, Amt für Volkswirtschaft, Amtsleiterin

— Dr. Marie-Louise Gächter-Alge, Datenschutzstelle Liechtenstein, Leiterin

— Prof. Dr. Pavel Laskov, Hilti Lehrstuhl für Daten- und Anwendungssicherheit, Institut für Wirtschaftsinformatik, Universität Liechtenstein

— Harald Oberdorfer, Amt für Justiz, Abteilung Justizwesen

— Patrik Marxer, Cyber Security Liechtenstein, Präsident Verein

— Dr. Daniel Miescher, Schulamt, Mittel- und Hochschulwesen

— Tino Quaderer, Gemeinde Eschen, Gemeindevorsteher, Delegierter Vorsteherkonferenz

— Jennifer Rheinberger, Amt für Soziale Dienste, Vorsitzende Fachgruppe Medienkompetenz

— Horst Schädler, Regierungssekretär

— Peter Sele, Regierungskanzlei

Interviewpartner
— SpeedCom AG, Andreas Kollmann, CEO

— LGT Financial Services AG, François Chapuis, CSO

— ARGUS Sicherheitsdienst AG, Daniel Banzer, Leiter Technik

— Liechtensteinische Kraftwerke, Gerald Marxer, CEO

— oerlikon balzers, Alessandra Doëll, Head of Communications; Raluca Voicu, Head of Business Development

— Telecom Liechtenstein AG, Aldo Frick, CEO, Pirol Bont, Mediensprecher

— Universität Liechtenstein, Pavel Laskov, Hilti Lehrstuhl für Daten- und Anwendungssicherheit, Institut für Wirtschaftsinformatik, Universität Liechtenstein

— Amt für Informatik, Patrik Thoma

— Amt für Kommunikation, Rainer Schnepfleitner

— Amt für Justiz, Harald Oberdorfer

— Datenschutzstelle, Marie-Louise Gächter

Weitere Gespräche wurden geführt mit

— S.D. Erbprinz Alois von und zu Liechtenstein

— Michael Schöb, Leiter Stabsstelle Financial Intelligence Unit (FIU)

— Dominik Häuptle, Finanzmarktaufsicht Liechtenstein (FMA), Stab der Geschäftsleitung, Leiter Recht/Internationales

— Dr. Robert Wallner, Leitender Staatsanwalt, Staatsanwaltschaft Liechtenstein

— Andreas Schädler, Chef Kriminalpolizei

Stellungnahmen im Zuge der Strategie-Erarbeitung erfolgten durch

— ENISA (European Union Agency for Cybersecurity / Agentur der Europäischen Union für Cybersicherheit), 20. Mai 2020

— Vorsteherkonferenz der liechtensteinischen Gemeinden, 29. Juni 2020

— Chief Information Security Officer der LGT Bank, VP Bank und Liechtensteinische Landesbank, 30. Juni 2020