Juli 2020

CYBER-SICHERHEIT IN LIECHTENSTEIN

Risiken, aktuelle Praxis und Handlungsbedarf

UNIVERSITÄT LIECHTENSTEIN

funk STIFTUNG

funk

FL

Im Auftrag von
digital-liechtenstein.li

Juli 2020

digital-liechtenstein.li

Impressum

Herausgeber:
digital-liechtenstein.li
Wuhrstrasse 7, 9490 Vaduz
www.digital-liechtenstein.li
info@digital-liechtenstein.li

Gestaltung:
Co-Agency Ltd.
Landstrasse 145, 9494 Schaan
www.co-agency.li
info@co-agency.li

Druck:
Wolf Druck AG
Schliessa 12, 9495 Triesen
www.wolf-druck.li
info@wolf-druck.li

Autoren der Studie:

Pavel Laskov
Professor, Inhaber des Hilti Lehrstuhls für Daten- und Anwendungssicherheit, Universität Liechtenstein

Frank Breitinger
Assistenzprofessor am Hilti Lehrstuhl für Daten- und Anwendungssicherheit, Universität Liechtenstein

Stefan Maag
Studierender im Masterstudiengang Wirtschafts-informatik, Universität Liechtenstein

Felix Salcher
Studierender im Masterstudiengang Wirtschafts-informatik, Universität Liechtenstein

Marc Schlömmer
Studierender im Masterstudiengang Wirtschafts-informatik, Universität Liechtenstein

Johannes Walter
Studierender im Masterstudiengang Wirtschafts-informatik, Universität Liechtenstein

Vorwort

Jedes zweite Unternehmen in Liechtenstein ist bereits Opfer eines Cyber-Angriffs geworden. Die folgende Studie der Universität Liechtenstein im Auftrag von digital-liechtenstein.li sieht ein hohes Risiko für den Wirtschaftsstandort. Staat und Wirtschaft sind gefordert, die Prävention von Cyberangriffen zu verbessern und die Sensibilisierung für Sicherheitsmassnahmen zu verstärken.

Cyber-Sicherheit gilt als unerlässliche Voraussetzung für den Erfolg der digitalen Transformation. Dies betrifft sowohl Grossunternehmen als auch KMU. Vor diesem Hintergrund hat digital-liechtenstein.li eine Studie in Auftrag gegeben, um die aktuelle Lage der Cyber-Sicherheit für den Wirtschaftsstandort Liechtenstein einzuschätzen.

Herzlichen Dank an dieser Stelle an das Institut für Wirtschaftsinformatik an der Universität Liechtenstein, welche unter der Federführung von Professor Pavel Laskov, Inhaber des Hilti Lehrstuhls für Daten- und Anwendungssicherheit, gemeinsam mit Studierenden diese Studie erarbeitet hat. Die Ergebnisse basieren auf einer repräsentativen Online-Umfrage bei über 100 Unternehmen sowie verschiedenen Verwaltungsstellen in Liechtenstein.

Teil der Kampagne „Cyber Security»

Die Studie ist wesentlicher Bestandteil der Kampagne Cyber Security, welche digital-liechtenstein.li im Herbst 2019 lanciert hat. Die Kampagne soll unter anderem das Bewusstsein für Cyber-Sicherheit schärfen und konkrete Hilfestellungen vor allem für KMU bieten. Dreh- und Angelpunkt der Kampagne ist die Webseite www.cybercheck.li, auf welcher Firmenverantwortliche einen kostenlosen Schnellcheck mit konkreten Handlungsempfehlungen machen und das finanzielle Risiko eines Cyberangriff kalkulieren können. Auch hat die Initiative bereits verschiedene Workshops und Veranstaltungen durchgeführt.

Die Beteiligten konnten die Ergebnisse der Studie am 25. Juni 2020 auf Schloss Vaduz präsentieren und gemeinsam mit Erbprinz Alois von und zu Liechtenstein diskutieren. Lothar Ritter, Vorsitzender des Boards von digital-liechtenstein.li: «Die Ergebnisse der Studie sollen zur Sensibilisierung von Politik und Wirtschaft beitragen. Es freut uns, dass unsere Initiative bereits einige Massnahmen in diesem Bereich umsetzen konnte und wir aktuell auch in der nationalen Strategie für Liechtenstein zum Schutz vor Cyber-Risiken aktiv mitwirken.» Erbprinz Alois sieht im Thema ebenfalls eine

Vertreter von digital-liechtenstein.li konnten die Ergebnisse der Studie am 25. Juni 2020 auf Schloss Vaduz präsentieren und gemeinsam mit Erbprinz Alois von und zu Liechtenstein diskutieren.

zentrale Herausforderung für Liechtenstein: «Die Pandemie hat in Bereichen wie Home Office und Home Schooling die grosse Bedeutung einer stabilen und sicheren Dateninfrastruktur für unsere heutige Gesellschaft gezeigt. Staat und Wirtschaft sollten daher beim Thema Cyber Security eine enge Zusammenarbeit sicherstellen.»

Die Studie wurde massgeblich unterstützt von der Funk Stiftung. Die Funk Stiftung fördert schwerpunktmässig wissenschaftliche und praxisbezogene Projekte rund um die Themen Risikoforschung und Risikobewältigung. «Die digitale Transformation setzt einen intensiven Umgang mit dem Thema Cyber Security voraus. Es freut uns, dass die Studie hierzu wesentliche empirische Erkenntnisse und daraus abzuleitende Handlungsempfehlungen liefert», sagt Stefanie Hillegaart, stellvertretende Vorstandsvorsitzende der Funk Stiftung.

Breit getragene Initiative

Die Standortinitiative digital-liechtenstein.li wurde Ende 2017 lanciert, um den Wirtschaftsstandort auf dem Weg ins digitale Zeitalter zu unterstützen. Die Initiative steht unter dem Patronat des Fürstenhauses und der Regierung und wird von rund 50 Unternehmen und Organisationen aus Wirtschaft, Wissenschaft und Politik getragen. digital-liechtenstein.li unterstützt die relevanten Akteure in der digitalen Innovation und Transformation. Bereits konnten zahlreiche Plattformen gegründet sowie Massnahmen und Aktivitäten lanciert werden. Spezielle Partner der Kampagne «Cyber Security Liechtenstein» sind die Funk-Gruppe, Funk Stiftung, FL1, die Universität Liechtenstein, BDO, die MTF Group, Speedcom und HSL Informatik.

Markus Goop & Patrick Stahl
Geschäftsführung digital-liechtenstein.li

Weiterführende Informationen und Download der Studie finden Sie auf: **www.digital-liechtenstein.li**

digital–liechtenstein.li

Einleitung

Cyber-Sicherheit gilt als eines der grössten «Sorgenkinder» der Digitalisierung. Die Erfahrungen der letzten zwei Jahrzehnte förderten zahlreiche Beispiele von enormen finanziellen, gesellschaftlichen, politischen sowie rufschädigenden Folgen zutage. «Geboren» als Zeichen von intellektueller Kreativität und Ehrgeiz, reicht heutige Hackertätigkeit weit über ein technisches Umfeld hinaus. Derzeitige Cyber-Angriffe haben verschiedenartige Zwecke, die zumeist wirtschaftlich motiviert sind. Hierzu zählen eine direkte Erpressung der Opfer, betrügerische Ausnutzung diverser Internetdienste, illegaler Handel mit gestohlenen Daten, Entwenden von Geschäftsgeheimnissen und Know-how, um nur ein paar Beispiele zu nennen. Darüber hinaus können Cyber-Angriffe als Instrument für Sabotage, Terrorismus oder gar militärische Handlung genutzt werden.

Liechtenstein verbindet wesentliche gesellschaftliche Ziele mit dem Fortschritt der Digitalisierung. In der 2019 von der Regierung des Fürstentums Liechtenstein verabschiedeten Digitalen Agenda werden die Grundprinzipien für die Entwicklung und Anwendung von digitalen Technologien in Liechtenstein festgelegt sowie die Bereiche mit priorisiertem Handlungsbedarf identifiziert. Hierzu zählen unter anderem E-Government, Bildung, Infrastruktur, Verkehr, Gesundheit, Kultur sowie diverse Wirtschaftsbranchen. Selbstverständlich ist die Gewährung von etablierten Sicherheitszielen Teil der Digitalen Agenda. Als wichtige Zielsetzung werden darin unter anderem Daten- und Informationssicherheit, Schutz von kritischen Infrastrukturen, internationale Vernetzung und Koordination auf dem Gebiet der Cyber-Sicherheit sowie sichere Identifikation und Authentifizierung genannt.

Die Planung und Umsetzung von Massnahmen auf dem Gebiet der Cyber-Sicherheit erfordern eine Bestandsauf-

nahme des aktuellen Status Quo. Zu diesem Zweck wurde diese Studie als repräsentative Umfrage der beteiligten Personen aus liechtensteinischer Industrie und Verwaltung konzipiert. Die Fragen, die wir an die Teilnehmer adressierten, dienen der Klärung von folgenden zwei Kernfragen:

» Wie ist der Wirtschaftsstandort Liechtenstein auf Cyber-Angriffe aus der Sicht von Unternehmen vorbereitet?
» Welche technischen und organisatorischen Massnahmen wenden Unternehmen an, um ihren Schutz gegen Cyber-Angriffe zu gewährleisten?

Durch die Auswertung der Antworten versuchen wir zu klären, ob die Lage in Bezug auf Cyber-Sicherheit in Liechtenstein im Wesentlichen mit bekannten Trends auf diesem Gebiet übereinstimmt und ob besondere Massnahmen erforderlich sind, um einen adäquaten Standard zu erreichen. Neben eigens erhobenen Daten werden hierzu gegebenenfalls Ergebnisse anderer ähnlicher Studien herangezogen.

Die gestellten Fragen orientieren sich an drei Themen, die für die Beurteilung der Cyber-Sicherheit in Liechtenstein von essentieller Bedeutung sind. Als erstes Thema gilt die Charakterisierung von Cyber-Risiken, denen Liechtensteiner Unternehmen ausgesetzt sind. Da die Schutzmassnahmen gegen Cyber-Angriffe in der Regel sehr kostspielig sind, muss deren Umsetzung nach Risiken priorisiert werden. Die Restrisiken können entweder von Unternehmen selbst oder durch den Abschluss geeigneter Versicherungen gegen Schäden durch Cyber-Angriffe abgedeckt werden. Das zweite Thema ist der aktuelle Stand der Praxis in der Cyber-Sicherheit in Liechtenstein. Diese Fragen ermitteln, ob bestimmte Massnahmen in Unternehmen umgesetzt sind. Durch den Abgleich vom Grad der Umsetzung einzelner Massnahmen mit festgestellten Risiken lassen sich als drittes Thema Handlungsempfehlungen erarbeiten. Hierzu wurden auch zusätzliche Fragen gestellt, welche die Meinung der Teilnehmer zu ausgewählten Handlungsschritten erforschen.

Aufgrund der Komplexität der Fragestellungen erfordert der Schutz vor Cyber-Angriffen eine Vernetzung diverser Akteure sowie umfassende und heterogene Kompetenzen. Die Universität Liechtenstein, deren Studierende und akademische Mitarbeiter gemeinsam mit der Initiative digital-liechtenstein.li diese Studie konzipiert und durchgeführt haben, arbeitet seit 2018 am Ausbau der wissenschaftlichen Kompetenzen auf dem Gebiet der Cyber-Sicherheit. Wir hoffen, dass die ermittelten Fakten sowie unsere Handlungsempfehlungen zu einem weiteren Austausch und einer fruchtbaren Zusammenarbeit auf dem spannenden Gebiet der Cyber-Sicherheit führen werden.

Konzeption und Durchführung der Studie

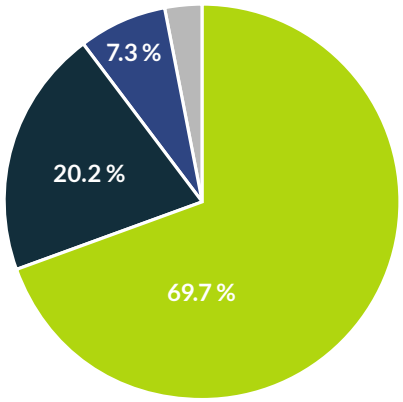
Der Fragebogen für eine Online-Umfrage wurde im Zeitraum Oktober/November 2019 an der Universität Liechtenstein in Abstimmung mit digital-liechtenstein.li entwickelt. Die Umfrage war an Geschäftsführung, IT-Verantwortliche sowie Mitarbeiter der IT-Abteilungen adressiert. Die Umfrage umfasste allgemeine, wirtschaftliche, organisatorische und technische Fragen. Um eine effiziente Verarbeitung der Antworten zu ermöglichen, wurden in der Studie generell Selektivfragen eingesetzt. Als Grundlage für die Analyse dienen dementsprechend die Anteile von bestimmten Antworten. Bei den meisten Fragen wurde auch die Möglichkeit vorgesehen, keine Antwort abzugeben. Je nach Frage kann dies zu unterschiedlichen Interpretationen führen.

Der Fragebogen wurde durch das Netzwerk von digital-liechtenstein.li und der Wirtschaftsverbände mittels unterschiedlicher Medien wie beispielsweise E-Mail und Newsletter breit gestreut. Anschliessend war die Teilnahme vom 21.11.2019 bis 31.01.2020 online möglich. Alle Angaben waren anonym und wurden von den beteiligten Parteien streng vertraulich behandelt. Insgesamt wurden 109 Antworten berücksichtigt.

Zur Profilierung der Teilnehmer bei gleichzeitiger Gewährung der Anonymität wurde lediglich nach der Position im Unternehmen sowie dessen Grösse gefragt. Die Teilnehmerprofile sind in der folgenden Tabelle (bzw. Diagramm) dargestellt:

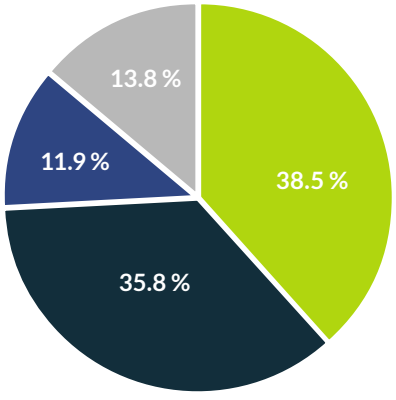
Was ist Ihre Position im Unternehmen?

Geschäftsleitung	69.7 %
IT-Abteilung	20.2 %
Sonstiges	7.3 %
Keine Angabe	2.8 %



Wie viele Mitarbeitende arbeiten in Ihrem Unternehmen?

0-9	38.5 %
10-49	35.8 %
50-249	11.9 %
250 oder höher	13.8 %

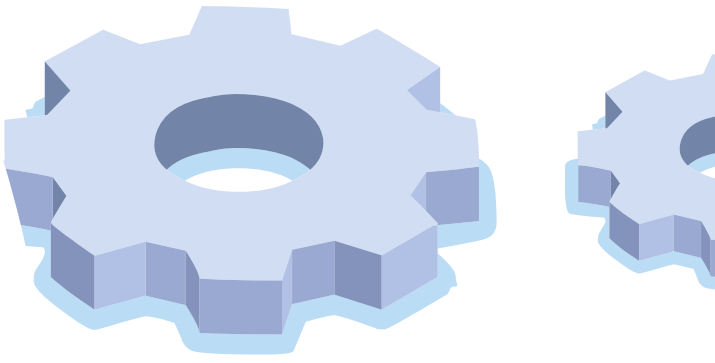


Der Grossteil (70 %) der Teilnehmer stammt aus der Geschäftsleitung, gefolgt von 20 % Beschäftigter in der IT-Abteilung. Die restlichen Teilnehmer machten entweder keine Angabe oder stammen aus anderen Bereichen wie beispielsweise Marketing, Führungsteam oder Operations. Im Hinblick auf die Unternehmensgrösse wurden vier Kategorien definiert: 0-9, 10-49, 50-249, und 250 oder höher. Wie es in Liechtenstein zu erwarten ist, stammt die Mehrheit der Teilnehmer aus kleineren Unternehmen. 39 % der befragten Unternehmen hatte weniger als 10 Mitarbeiter, gefolgt von 36 %, die zwischen 10 und 49 Mitarbeiter beschäftigten.

Wie bereits erwähnt, wurden bei der Gestaltung der Umfrage Selektivfragen bevorzugt. Je nach Semantik der Frage wurden kategorische Aussagen auf der Skala 1 (trifft gar nicht zu) bis 5 (trifft voll zu) gemessen oder Ja/Nein Antworten angeboten. Bei einer Frage wurden Teilnehmer gebeten, Ihre «Budgets» prozentual in 5 verschiedene Bereiche aufzuteilen.

Die Auswertung der Ergebnisse basiert auf einer qualitativen Analyse der Anteile verschiedener Antworten. Da die Stichprobe von 109 Datensätzen statistisch gesehen vergleichsweise gering ist, wurden keine statistischen Tests durchgeführt. Bei Bedarf wurde bei einigen Fragen eine Profilierung von Antworten nach der Unternehmensgrösse untersucht. Da die Aufteilung von Teilnehmern nach Position eher einseitig war (überwiegend Geschäftsführung) wurde keine Profilierung der Antworten nach Position durchgeführt.

Die Ergebnisse der Studie werden in der folgenden Darstellung in drei Themen aufgeteilt. Zunächst werden die Antworten zu Fragen mit Bezug auf Cyber-Risiken analysiert, gefolgt von Fragen zum aktuellen Stand der Praxis und schliesslich die unmittelbar für die Handlungsempfehlungen relevanten Fragen. Diese Aufteilung wurde nachträglich zu Analysezwecken eingeführt. In der Online-Umfrage wurden die Fragen in einer anderen Reihenfolge gestellt und die Teilnehmer waren sich dementsprechend dieser Logik der Analyse nicht bewusst.

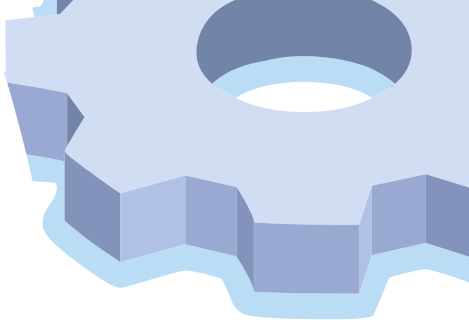


Einschätzung der aktuellen Cyber-Risiken

Dieser Abschnitt beinhaltet allgemeine Fragen, die mit aktuellen Cyber-Risiken zusammenhängen. Die Antworten basieren auf der Eigeneinschätzung der Teilnehmer. Die Fragen zielen entweder auf die Gesamtlage in Liechtenstein oder auf die Lage im Unternehmen. Eine Übersicht der Ergebnisse ist in den untenstehenden Tabellen aufgeführt. In der ersten Tabelle sind Fragen mit kategorischen Antworten und in der zweiten Tabelle die Fragen mit Ja/Nein Antworten dargestellt. Für beide Arten von Fragen bestand eine Option, keine Antwort (KA) abzugeben.

1 = Trifft gar nicht zu / 5 = Trifft voll zu	1	2	3	4	5	KA
Es besteht ein hohes Risiko für Unternehmen in Liechtenstein Opfer eines Cyber-Angriffs zu werden	0.9	5.5	26.6	34.9	27.5	4.6
Ihr Unternehmen ist ein potenzielles Ziel für einen Cyber-Angriff	11.0	27.5	20.2	17.4	21.1	2.8
IT-Sicherheit ist ein wichtiges Thema in Ihrem Unternehmen	0.0	6.4	11.0	25.7	56.9	0.0
Ein Cyber-Angriff würde Ihre leistungserbringenden Prozesse lahmlegen und somit die Geschäftsfähigkeit massgeblich beeinträchtigen	0.9	11.0	17.4	30.3	39.4	0.9
Ihr Unternehmen wird sich die nächsten zwei Jahren verstärkt mit dem Ausbau der Cyber-Sicherheit beschäftigen	2.8	13.8	28.4	25.7	28.4	0.9
Ihr Unternehmen ist gut gegen einen Cyber-Angriff geschützt	2.8	9.2	17.4	47.7	20.2	2.8
Ihr Unternehmen ist gegen mögliche Schäden durch Cyber-Angriffe versichert	36.7	11.0	8.3	7.3	23.9	12.8

	Ja	Nein
Ihr Unternehmen wurde bereits Ziel eines Cyber-Angriffs	54.1	49.9
... eines Denial-of-Service-Angriffs	15.6	84.4
... eines Malware-Angriffs	25.7	74.3
... eines Phishing-Angriffs	39.4	60.6
... eines Ransomware-Angriffs	10.1	89.9
... eines Datendiebstahls	11.0	89.0
... eines Insider-Angriffs	4.6	95.4
... eines anderen Angriffs	10.1	89.9



Analyse der Ergebnisse

Die Bedrohungen durch Cyber-Angriffe steigen von Jahr zu Jahr und somit auch die Bedeutung von IT-Experten für Unternehmen. Einige frühere Studien befassten sich mit der Einschätzung der aktuellen Bedrohungslage. Zum Beispiel berichtet der Eco-Verband der Internetwirtschaft in der IT-Sicherheitsstudie 2020, dass «über 90 Prozent der IT-Experten in Deutschland die allgemeine Bedrohungslage bei der Internet-Sicherheit als wachsend einschätzt».

Die ersten beiden Fragen unserer Studie zu aktuellen Cyber-Risiken befassen sich mit der Risiko-Wahrnehmung der Liechtensteiner Unternehmen. Hierbei unterscheiden wir zwischen «Unternehmen im Land» und «eigenes Unternehmen». Sehen Führungskräfte / Verantwortliche ein hohes Risiko, so ist dies unter Umständen positiv zu werten, da dies eine Bereitschaft signalisiert, entsprechende organisatorische Massnahmen einzuführen sowie finanzielle Mittel zur Verfügung zu stellen. Diese beiden Arten von Entscheidungen führen zum besseren Schutz des Unternehmens.

Die Ergebnisse zeigen, dass eine grosse Mehrheit der Befragten ein hohes Risiko für Unternehmen in Liechtenstein sieht, Opfer eines Cyber-Angriffs zu werden. Im Einzelnen bewerten 89 % das Risiko für Unternehmen in Liechtenstein mit mittel bis sehr hoch. Somit stimmt dieses Ergebnis vollkommen mit der Eco-Studie in Deutschland überein.

Interessanterweise wird das Risiko für das eigene Unternehmen deutlich geringer eingeschätzt. Hier schätzen nur 59 % der Befragten das Risiko zwischen mittel bis sehr hoch. Diese Diskrepanz liegt an unterschiedlichen Wahrnehmungen bei grossen (>=250), mittleren (50-249) und kleineren Unternehmen. Bei grossen Unternehmen ist die allgemeine Risikowahrnehmung in Liechtenstein mit der Risikowahrnehmung für das Unternehmen identisch (93 % hoch und sehr hoch). Bei mittleren Unternehmen schätzen 85 % das Risiko für Liechtenstein aber lediglich 45 % für ihr eigenes Unternehmen als hoch und sehr hoch ein. Bei kleineren Unternehmen ist die Risikowahrnehmung grundsätzlich geringer. Nur 53 % der Befragten in dieser Kategorie schätzen das Risiko für Liechtenstein und nur 27 % für ihr Unternehmen als hoch und sehr hoch ein. Diese Erkenntnisse offenbaren zwei unterschiedliche Phänomene. Zum einen mögen kleinere Unternehmen in der Tat aufgrund ihrer Geschäftsmodelle geringeren Cyber-Risiken ausgesetzt sein. Für Kriminelle rentieren sich besonders raffinierte Angriffe auf kleinere Unternehmen meist nicht. Als zweites Phänomen ist bei dieser Analyse eindeutig die «Warum ich?» Haltung zu erkennen, was sich sowohl in der Wahrnehmung von eigenen Cyber-Risiken als auch in der Einschätzung von Risiken für Liechtenstein niederschlägt.

Überraschend einig waren sich die Teilnehmer, dass Cyber-Sicherheit ein wichtiges Thema in ihrem Unternehmen ist, auch wenn die Gefahr für ein eigenes Unternehmen als gering oder mittel eingeschätzt wird. Bei grossen Unternehmen liegt der Anteil der Bewertungen mit 4 und 5 bei 100 %, bei allen anderen zwischen 75 % und 85 %. Dieses Ergebnis zeigt, dass die meisten Liechtensteiner Unternehmen sich der Bedeutung der Cyber-Sicherheit sehr bewusst sind.

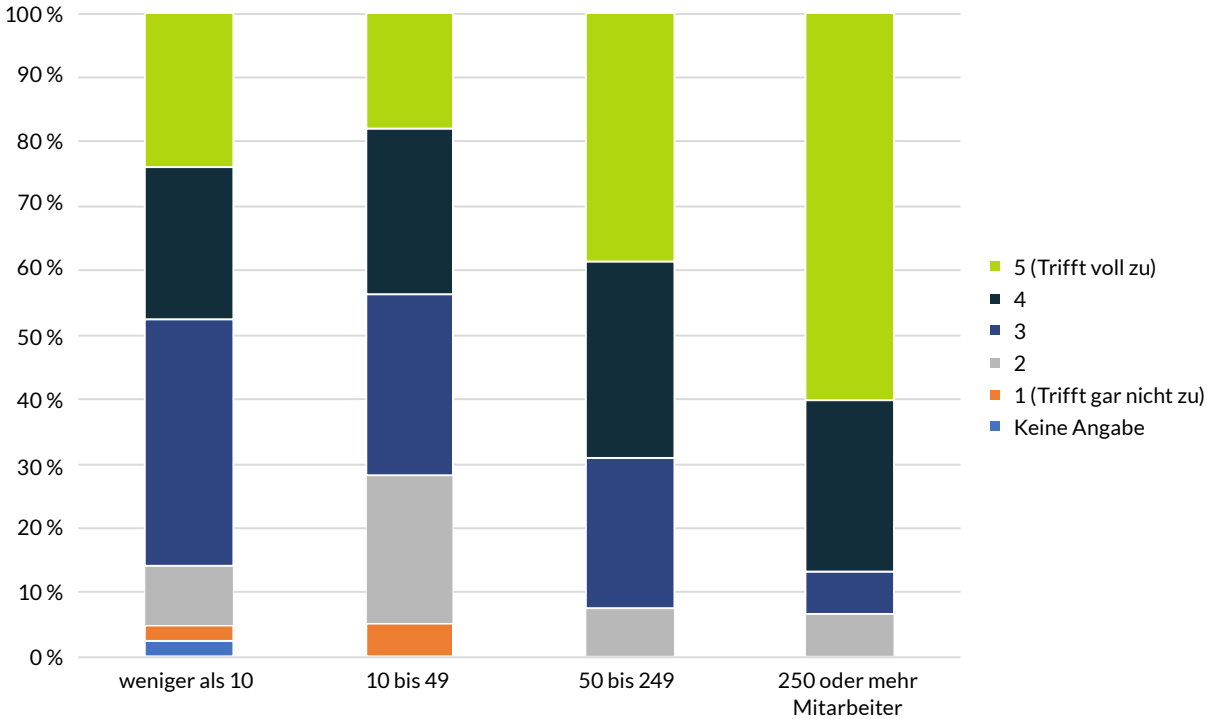
Ein möglicher Grund für das Bewusstsein über die hohe Bedeutung der Cyber-Sicherheit kann darin liegen, dass Cyber-Angriffe häufig kritische Geschäftsprozesse lahmlegen und somit die Geschäftsfähigkeit massgeblich beeinträchtigen. Dies ist oft der Fall bei Ransomware-Angriffen, bei denen alle Daten verschlüsselt werden und der Zugriff auf Systeme / Daten nicht mehr oder nur sehr eingeschränkt möglich ist. Oft wird übersehen, dass ein Angriff meist nicht einen einzelnen Rechner lahmlegt, sondern sich im Netzwerk verbreitet

und daran angeschlossene Geräte anfallen kann, z. B. Telefonanlagen, IoT-Geräte, Mobiltelefone oder Steuerungsanlagen. Neben Ransomware können auch andere Angriffe gravierende existenzbedrohliche Schäden verursachen, beispielsweise, s. g. «Denial-of-Service» Angriffe auf Unternehmen, deren Geschäfte in Echtzeit über Internet abgewickelt werden (E-Commerce, Online-Spiele, Streaming-Dienste, usw.).

Knapp 70 % der Befragten stimmten zu, dass erfolgreiche Cyber-Angriffe leistungserbringende Prozesse lahmlegen und somit die Geschäftsfähigkeit massgeblich beeinträchtigen können. Weitere 17 % räumten zumindest mittelmässige Auswirkungen ein, gefolgt von 12 %, die Beeinträchtigungen für gering halten. Bei dieser Frage ist auch erkennbar, dass je grösser das Unternehmen ist, desto stärker der Einfluss der Cyber-Angriffe auf kritische Geschäftsprozesse wahrgenommen wird.

Die Bereitschaft der Unternehmen, sich in der näheren Zukunft mit Fragen der Cyber-Sicherheit zu beschäftigen, ist offenkundig auch eng mit den steigenden Cyber-Risiken verbunden. 54 % der Befragten schätzen, dass ihr Unternehmen sich in den nächsten zwei Jahren in hohem oder sehr hohem Masse mit dem Ausbau der Cyber-Sicherheit beschäftigen wird. Die Verteilung der Antworten auf diese Frage nach Unternehmensgrösse (siehe Grafik unten) ist sehr aufschlussreich. Den stärksten Ausbau der IT-Sicherheit erwarten die grossen Unternehmen (86 % von hoch und sehr hoch). Das ist nachvollziehbar, da diese den höchsten Risiken ausgesetzt sind und über substanzielle Ressourcen für einen solchen Ausbau verfügen. Bei den zwei nächstkleineren Kategorien der Unternehmen ist ein deutlich geringeres Mass für den Ausbau der Cyber-Sicherheit zu erwarten, so geben beispielsweise 23 % der Befragten aus Unternehmen mit 10-49 Mitarbeitern an, dass sie einen geringen Ausbau erwarten. Bei Kleinstunternehmen steigt die erwartete Auseinandersetzung mit Themen der Cyber-Sicherheit wieder deutlich an, mit etwa 86 % der Antworten in Kategorien mittel bis sehr hoch. Dieser Effekt ist am wahrscheinlichsten mit der Tatsache verbunden, dass die kleinsten Unternehmen einen grossen Nachholbedarf auf diesem Gebiet sehen, weil bei ihnen die Cyber-Sicherheit bisher nicht ausreichend adressiert wurde.

Ihr Unternehmen wird sich die nächsten zwei Jahren verstärkt mit dem Ausbau der Cyber-Sicherheit beschäftigen.



Eine wesentliche Frage in unserer Analyse der Cyber-Risiken ist, wie gut sich die Unternehmen gegen Cyber-Angriffe geschützt fühlen. Diese Frage ist bewusst subjektiv gestellt. Eine objektive Schätzung des Schutzniveaus ist sehr aufwendig und kann nicht flächendeckend durchgeführt werden. Die in unserer Studie durchgeführte subjektive Schätzung lässt nicht nur eine objektive Schätzung annähern, sondern auch potentielle Entscheidungen in Bezug auf weitere Massnahmen nachvollziehen.

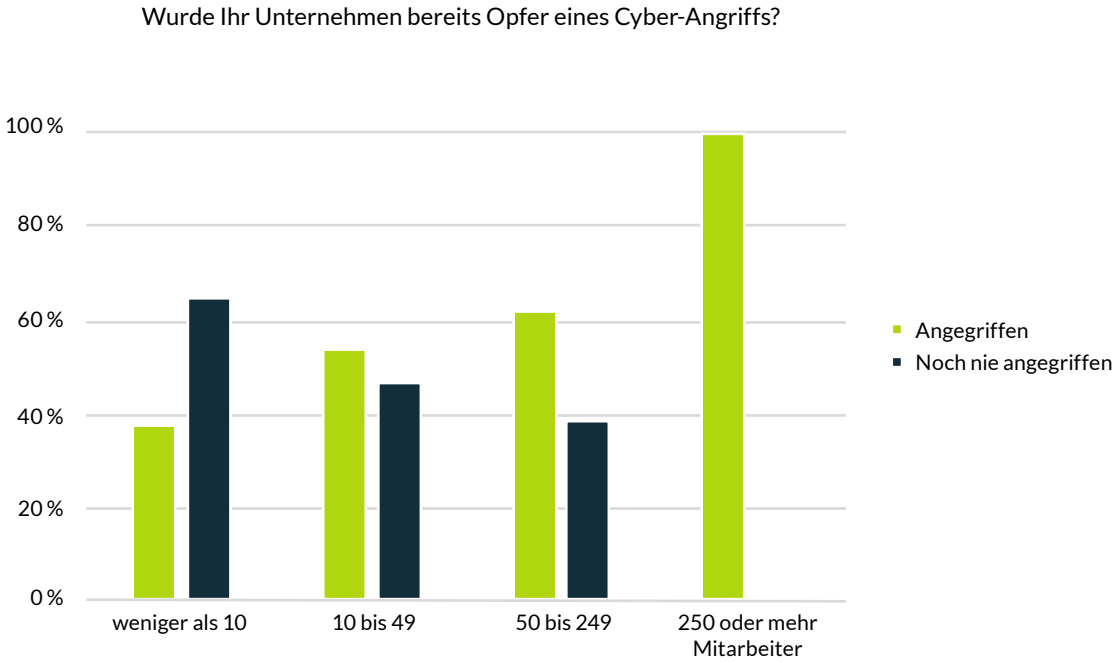
Die meisten beteiligten Unternehmen schätzen die aktuelle Sicherheitslage und Vorkehrungen positiv ein. Im Detail gaben 20 % der Befragten an, dass ihr Unternehmen sehr gut gegen einen Cyber-Angriff geschützt ist. 48 % der Befragten empfinden einen guten Schutz. Die «durchschnittliche Meinung» aller Befragten ist «gut»: diese Antwort wählten rund die Hälfte aller Befragten ungeachtet der Unternehmensgrösse. Im nächsten Teil von diesem Kapitel versuchen wir zu klären, wie realistisch diese Einschätzung ist.

Können sich Unternehmen gegen Cyber-Risiken zuverlässig versichern? Generell spielen in heutiger Wirtschaft Versicherungen sowohl für Privatpersonen als auch für Unternehmen eine sehr bedeutende Rolle. Für viele Prozesse ist die Verteilung von Risiken durch eine Versicherung auf eine breite Basis der Teilnehmer ein zentrales Instrument zum Handeln in ungewisser Lage. Gilt dieses Instrument für Cyber-Risiken? Wenn ja, wird es breit eingesetzt? Aktuelle Cyber-Versicherungen erlauben sehr variable Modelle, die beispielsweise vor Datenschutzverletzungen (z. B. Verlust von Kundendaten) oder Betriebsunterbrechung durch Cyber-Angriffe schützen. Manche Versicherungen setzen jedoch Zertifizierungen wie ISO 27001 voraus, die sehr kostspielig sein können.

Aus unserer Umfrage ergibt sich kein homogenes Stimmungsbild zum Einsatz von Cyber-Versicherungen in Liechtenstein. Die meisten Antworten konzentrieren sich auf die extremen Werte (24 % sehr hoch und 37 % sehr gering, was vielleicht auch an der etwas binären Natur der Frage liegt). Darüber hinaus ergibt sich, dass bei kleineren Unternehmen (bis 49 Mitarbeiter) eine klare Mehrzahl (43 %) nicht gegen Cyber-Risiken versichert ist. Bei grösseren Unternehmen ist das Verhältnis anders, mit 39 % positiver Antworten («sehr hoch»). Diese Verteilung zeigt, dass aktuelle Versicherungsangebote tendenziell nicht auf die breite Basis der Unternehmen zugeschnitten sind. Das ist eigentlich schade, denn gerade die kleineren Unternehmen mit geringem fachlichem Know-how könnten von adäquaten Angeboten profitieren.

Im letzten Teil von diesem Kapitel werden die Fragen zu bereits erlittenen Sicherheitsvorfällen untersucht. Diese Fragen wurden als Ja/Nein Fragen zu ausgewählten Arten von Cyber-Angriffen definiert. Die dadurch ermittelten Zahlen spiegeln lediglich die erkannten Angriffe wider; sie verschaffen dennoch einen wertvollen Überblick über das Gesamtrisiko von Sicherheitsvorfällen sowie über spezifische Bedrohungen.

Allgemein waren 54 % der Befragten bereits Opfer mindestens eines Cyber-Angriffs. Die drei häufigsten Angriffsarten waren Phishing (39 %) sowie Malware (26 %) und Denial-of-Service (16 %). Datendiebstahl, Ransomware sowie «Andere» fielen mit jeweils ca. 10 % deutlich geringer aus. Für die Kategorie «Andere» wurden gehackte Benutzerkonten bzw. Webseiten genannt. Lediglich 5 % beklagten Insider-Bedrohungen. Diese Erkenntnisse legen nahe, dass das Gesamtrisiko von Sicherheitsvorfällen in Liechtenstein mit über 50 % sehr hoch ist. Auch wenn Schäden durch Phishing-Angriffe erfahrungsgemäss durch organisatorische Massnahmen in Grenzen gehalten werden, stellen die ermittelten Häufigkeiten der Angriffe durch Malware, Ransomware und Datendiebstahl ein erhebliches Risiko dar. Die in der folgenden Abbildung gezeigte Verteilung der Angriffshäufigkeit nach Unternehmensgrösse offenbart klar, dass der Grad der Betroffenheit durch Cyber-Angriffe deutlich mit der Grösse des Unternehmens ansteigt. Folglich belegen diese Erkenntnisse eher die Wahrnehmung von hohem Risiko in Liechtenstein als die Wahrnehmung von relativ geringem Risiko für einzelne Unternehmen sowie vom relativ guten Schutzniveau bei einzelnen Unternehmen.



Zusammenfassung

Aus der in diesem Kapitel vorgestellten Untersuchung von Cyber-Risiken in liechtensteinischer Wirtschaft können folgende Aspekte hervorgehoben werden:

1. Die Analyse von in dieser Umfrage gemeldeten Sicherheitsvorfällen deutet auf ein hohes Cyber-Risiko hin. Dieses Risiko wird im Allgemeinen richtig wahrgenommen, jedoch wird es in Bezug auf das eigene Unternehmen unterschätzt, vor allem bei kleineren Unternehmen.
2. Das Sicherheitsniveau im eigenen Unternehmen wird tendenziell überschätzt. Insbesondere grössere Unternehmen sind nicht allzu selten gefährlichen Angriffen wie Ransomware und Datendiebstahl ausgesetzt.
3. In Anbetracht des hohen Cyber-Risikos ist es sehr lobenswert, dass ein Grossteil der befragten Unternehmen plant, sich in den kommenden zwei Jahren verstärkt mit Cyber-Sicherheit zu beschäftigen.
4. Der Anteil von in Anspruch genommenen Cyber-Versicherungen ist tendenziell gering. Insbesondere kleinere Unternehmen werden von vorhandenen Produkten nicht ausreichend angesprochen.

Aktueller Stand der Praxis

Im folgenden Kapitel werden Ergebnisse vorgestellt, die Rückschlüsse auf einen aktuellen Stand der Praxis ermöglichen. Die Fragen in diesem Bereich ermitteln, wie gut die Sicherheitsmassnahmen zum Schutz vor Cyber-Angriffen in Liechtensteiner Unternehmen in der Praxis umgesetzt sind. Eine Übersicht der Ergebnisse ist in den untenstehenden Tabellen aufgeführt.

	Ja	Nein	KA
Die IT-Infrastruktur Ihres Unternehmens ist aktuell und dokumentiert.	82.6	12.8	4.6
Updates und Sicherheitspatches werden in Ihrem Unternehmen regelmässig eingespielt.	89.9	5.5	4.6
Die Benutzerberechtigungen in Ihrem Unternehmen basieren auf der jeweiligen Benutzerrolle, die von einer zentralen Stelle verwaltet wird.	81.7	10.1	8.3
Die Endgeräte in Ihrem Unternehmen unterliegen einem zentralen Management und einer Konfigurationsüberwachung.	66.1	22.9	11.0
In Ihrem Unternehmen gibt es eine Backup-Strategie.	93.6	2.8	3.7
In Ihrem Unternehmen sind die Backups physisch vom System getrennt.	84.4	5.5	10.1
In Ihrem Unternehmen gibt es einen Disaster Recovery Plan.	47.7	30.3	22.0
In Ihrem Unternehmen gibt es einen Business Continuity Plan.	38.5	41.3	20.2

	Ja	Nein	KA
Wird einer der folgenden Services in Ihrem Unternehmen extern betrieben?			9.2
… Datenspeicherung	54.1	45.9	
… Datenverarbeitung	30.3	69.7	
… IT-Sicherheitsdienstleistungen	44.0	56.0	
… Keiner von diesen Services	24.8	75.2	

1 = Trifft gar nicht zu / 5 = Trifft voll zu	1	2	3	4	5	KA
Es gibt einen IT-Prozess für das Ausscheiden einer/s Mitarbeitenden (z. B. Löschung von Zugriffsberechtigungen und Zugangsdaten)	18.4	8.3	6.4	16.5	44.0	6.4

Analyse der Ergebnisse

Die Grundlage für jegliche Massnahmen im Bereich von IT-Sicherheit ist eine ausführliche, vollständige und aktuelle Dokumentation der Systeme. Diese Grundlage wird benötigt, um potentielle Angriffsziele zu identifizieren und zu eliminieren und ermöglicht es vor allem externen Beratern, einen schnellen und kompletten Überblick über die IT-Sicherheitslage eines Unternehmens zu bekommen.
Die Ergebnisse unserer Umfrage zeigen, dass fast 83 % der befragten Unternehmen eine aktuelle Dokumentation ihrer IT-Infrastruktur besitzen. Hier gibt es keine signifikanten Unterschiede zwischen den einzelnen Unternehmensgrössen. Dies ist darauf zurückzuführen, dass mit steigender IT-Komplexität auch die Ressourcen steigen, die für die Dokumentation zur Verfügung stehen, steigen.

Eine der einfachsten und ertragreichsten Sicherheitsmassnahmen in der Verteidigung gegen Angriffe auf die eigenen IT-Systeme ist das regelmässige Einspielen von Updates und Sicherheitspatches für die komplette IT-Infrastruktur des Unternehmens. Diese Massnahme stellt sicher, dass Angreifer keine Möglichkeit haben, bekannte Schwachstellen auszunutzen, um Zugriff auf interne Systeme zu erhalten.

In dieser Hinsicht zeigen sich die Unternehmen Liechtensteins vorbildlich: 90 % aller befragten Unternehmen gaben an, Updates und Sicherheitspatches regelmässig und zeitnah in ihre Systeme einzuspielen. In Unternehmen mit über 250 Mitarbeitern haben sogar alle Unternehmen angegeben, dass sie diese Massnahmen konsequent umsetzen.

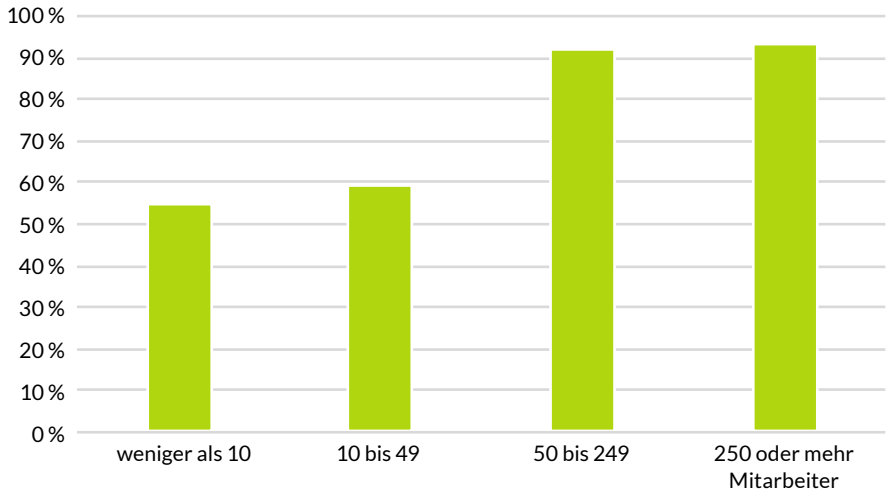
Die Benutzerberechtigungen für die einzelnen Accounts können auch ein erhebliches Sicherheitsrisiko darstellen. Über die Benutzerberechtigungen werden die Zugriffsregeln auf Daten für einzelne Benutzer oder Benutzergruppen festgelegt. Diese entscheiden darüber, ob ein Benutzer oder eine Benutzergruppe Berechtigungen wie Lesen, Schreiben oder Ausführen auf einen Datensatz hat oder nicht. Um sicherzustellen, dass nur die Personen auf Daten zugreifen können, für welche die Daten auch vorgesehen sind, ist eine zentrale Verwaltung der Benutzerberechtigungen enorm wichtig. Benutzerberechtigungen sollten basierend auf der Funktion des Mitarbeiters im Unternehmen vergeben und stets von einer zentralen Stelle verwaltet werden.

Die Umfrage hat ergeben, dass 82 % der Liechtensteiner Unternehmen diese Kriterien erfüllen. Auffallend dabei ist, dass auch hier alle Unternehmen mit über 250 Mitarbeitern über eine zentrale Verwaltung der Benutzerberechtigungen verfügen. Bei kleineren Unternehmen (weniger als 10 Mitarbeitern) ist dies bei über 19 % der befragten Unternehmen nicht der Fall.

Um zu verhindern, dass Schwachstellen, Sicherheitslücken und Fehlkonfigurationen auf Endgeräten als Einfallstore dienen, sollten alle Endgeräte im Unternehmen einem zentralen Management und einer Konfigurationsüberwachung unterliegen. Damit kann vorsorglich ein bestimmter Standard angestrebt werden, der von allen Endgeräten erfüllt werden muss, wenn diese für unternehmerische Tätigkeiten genutzt werden.

Bei Unternehmen mit unter 50 Mitarbeitern verfügen weniger als zwei Drittel der Befragten über ein zentrales Management und eine Konfigurationsüberwachung der Endgeräte. Bei den grösseren Unternehmen, mit mehr als 50 Mitarbeitern, sind es über 92 %, welche über ein zentrales Management und eine Konfigurationsüberwachung der Endgeräte verfügen.

Die Endgeräte im Unternehmen unterliegen einem zentralen Management und einer Konfigurationsüberwachung



Die Datensicherung mit der Absicht, im Verlustfall eine Sicherungskopie für die Datenwiederherstellung bereit zu haben, ist eine fundamentale Grundlage zur Datensicherheit in modernen Unternehmen. Aus diesem Grund wurden alle Unternehmen gefragt, ob es eine Backup-Strategie für die Unternehmensdaten gibt. Die Auswertung der Umfrage zeigt die Wichtigkeit von Backups bei Liechtensteiner Unternehmen klar auf. Rund 94 % der Befragten haben eine Backup-Strategie im Einsatz.

Somit kann argumentiert werden, dass Unternehmen sich der Wichtigkeit ihrer Datensicherheit bzw. der Auswirkungen eines Verlustes von Daten, die nicht redundant gesichert und wiederherstellbar sind, bewusst sind. Liechtensteiner Unternehmen sind im Fall eines Datenverlusts grösstenteils durch Backups geschützt. Es kann kein Zusammenhang zwischen Unternehmensgrösse und dem Erstellen eines Backups erkannt werden.

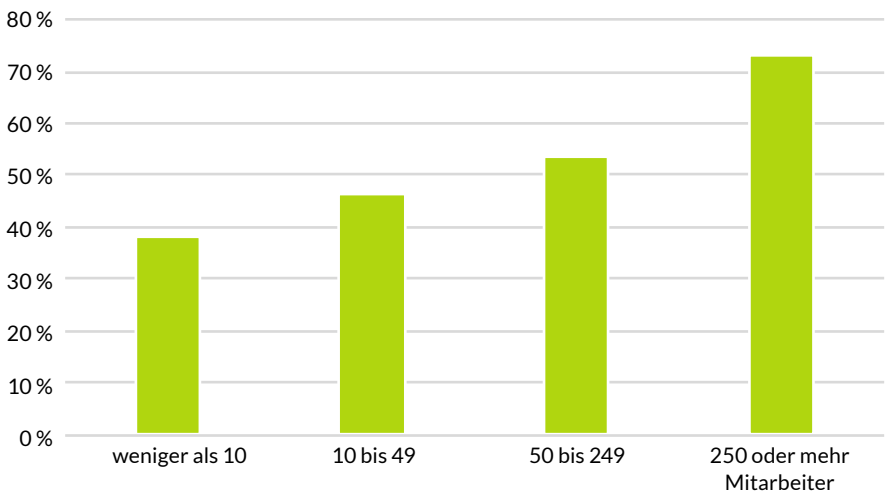
Die kritische Rolle von Backups als Instrument für die Gewährung von Datenintegrität wurde auch von den Angreifern erkannt. Demzufolge streben einige Ransomware-Angriffe auch die Zerstörung von Backups an. Sind Backup-Systeme über Netzwerke von befallenen Rechnern erreichbar, ist es in der Regel relativ einfach, für Schadsoftware den Zugriff auf Backups zu erlangen. Deswegen wird heute eine physische Trennung von Backup-Systemen und der übrigen IT-Infrastruktur empfohlen. Dies bringt zwar einen höheren Arbeitsaufwand für die Herstellung von Backups, schliesst aber nach einer Kompromittierung des Systems einen vollständigen Datenverlust aus.

Die Ergebnisse der Umfrage zeigen, dass diese Schutzmassnahme bei 84 % der Unternehmen umgesetzt wird. Somit kann beim Grossteil der Unternehmen ein Schutz des Backups durch physische Trennung sichergestellt werden.

Neben klassischen Backups ist ein Disaster Recovery Plan ein wichtiger Bestandteil der Sicherheitsstrategie eines Unternehmens. Ein Disaster Recovery Plan ist ein für Katastrophenfälle dokumentierter Prozess bzw. eine Reihe von Abläufen zur Wiederherstellung der Organisation und dem Schutz der IT-Infrastruktur eines Unternehmens. Es handelt sich hierbei um Massnahmen, die während einer ausserordentlichen Situation durchzuführen sind. Circa die Hälfte (48 %) der befragten Liechtensteiner Unternehmen besitzen einen Disaster Recovery Plan, während 22 % der Befragten keine Angaben zu dieser Frage machten.

Anhand der ausgewerteten Daten lässt sich erkennen, dass die Wahrscheinlichkeit der Verwendung eines Disaster Recovery Plans mit der Grösse des Unternehmens zunimmt. Lediglich 38 % der Unternehmen mit weniger als 10 Mitarbeitern haben einen Disaster Recovery Plan im Einsatz, während diese Zahl bei Unternehmen mit mehr als 250 Mitarbeitern auf 73 % ansteigt.

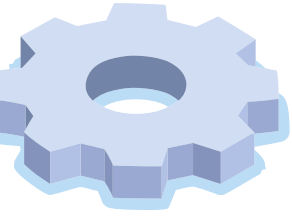
Im Unternehmen gibt es einen Disaster Recovery Plan.

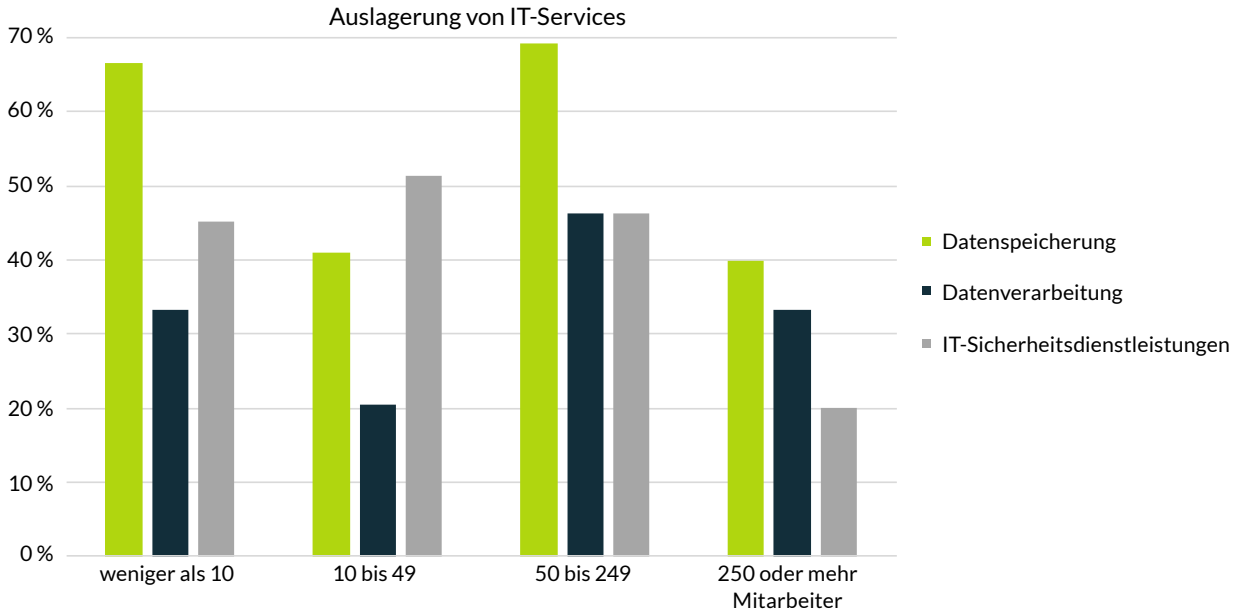


Zusätzlich zum Disaster Recovery Plan wurden die Teilnehmer auch zu ihrem Business Continuity Plan befragt. Im Unterschied zu einem Disaster Recovery Plan geht es beim Business Continuity Plan primär um die unmittelbare Fortführung der wichtigsten Unternehmensprozesse. In den meisten Unternehmen sind die Kernprozesse stark mit der IT-Infrastruktur verwoben und von dieser abhängig. Es ist daher wichtig, sich nicht nur damit zu beschäftigen wie das Unternehmen langfristig wieder auf die Beine gebracht werden kann, sondern sich auch Gedanken darüber zu machen, wie man den Ausfall der Kernprozesse so kurz wie möglich halten kann. In den Ergebnissen der Umfrage zeigt sich allerdings, dass sich weniger als die Hälfte (39 %) bereits mit dieser Thematik beschäftigt hat. Etwas mehr als 20 % der Unternehmen haben diese Frage mit «Keine Angabe» beantwortet, was eventuell darauf zurückzuführen ist, dass diese Massnahme den Befragten unbekannt war.

Im letzten Jahrzehnt zeichnet sich ein deutlicher Trend zur Auslagerung diverser IT-Dienste in die Cloud ab. Dies ermöglicht es Unternehmen, ihre IT-Kapazität besser an aktuelle Bedürfnisse anzupassen und ist insbesondere bei einem Mangel an qualifiziertem Personal eine sinnvolle Alternative zum Betrieb einer eigenen IT-Infrastruktur. Aus Sicht der Cyber-Sicherheit ist die Auslagerung von Diensten in die Cloud eine umstrittene Massnahme. Einerseits wird bei Inanspruchnahme von Cloud-Diensten auch die Verantwortung für deren sicheren Betrieb an die Dienstanbieter übertragen. Andererseits steigt dabei häufig die Komplexität der Authentifizierung massiv und es entstehen weitere Probleme bei Aufklärung der Sicherheitsvorfälle.

Bei unserer Befragung wurde untersucht, ob Unternehmen die Aufgaben der Datenspeicherung, Datenverarbeitung und IT-Sicherheit extern beziehen. Durch das Verlagern von IT-Services werden die Aufgaben an Unternehmen weitergegeben, welche sich auf diese Kompetenzen spezialisiert haben und daher in der Regel eine kostenattraktive Lösung anbieten können. 66 % beziehen mindestens einen der obigen Dienste von einem externen Partner und 17 % beziehen externe Services aus allen drei Bereichen. Interessant dabei ist, dass im Vergleich zu 26 % bei Unternehmen mit weniger als zehn Mitarbeitenden, 60 % der Unternehmen mit 250 oder mehr Mitarbeitenden alle drei Bereiche intern abwickeln. Bei der separaten Betrachtung der Services fällt auf, dass die Datenspeicherung mit durchschnittlich 54 % der am meisten extern beanspruchte Service ist. Auch die IT-Sicherheitsdienstleistung wird von den Unternehmen zu 44 % ausgelagert. Die Datenverarbeitung bleibt jedoch grösstenteils intern im Unternehmen und wird durchschnittlich nur zu 30 % extern betrieben.





Neben den operativen Diensten wie Datenspeicherung oder -verarbeitung können auch die mit der Cyber-Sicherheit verbundenen Aufgaben an externe Dienstleister ausgelagert werden. Diese Dienste sind in der Praxis als «Managed Security Service» bekannt und umfassen in der Regel den Betrieb von Firewalls und Proxies sowie die Überwachung von sicherheitsrelevanten Ereignissen. Aus unserer Umfrage ergibt sich, dass 44 % der Unternehmen die IT-Sicherheit als Service ausgelagert haben. Es ist dabei ein klarer Unterschied bei der Unternehmensgrösse zu erkennen. Die Daten zeigen, dass vor allem Unternehmen mit mehr als 250 Mitarbeitern IT-Sicherheit intern betreiben: 80 % der Grossunternehmen gaben dies an.

Fast jeder Mitarbeiter eines Unternehmens besitzt ein Benutzerkonto im intern verwendeten IT-System. Ausserdem stellen Unternehmen Hardware wie Laptops, Firmenhandys und Headsets, falls für die Ausübung der beruflichen Tätigkeit notwendig, zur Verfügung. Verlässt ein Mitarbeitender das Unternehmen, wird dieses Benutzerkonto und die mit dem Konto verbundenen Zugriffsrechte auf Dateisysteme, Firmen E-Mail usw. nicht mehr benötigt. Damit es keine ungewollten Zugriffe auf Systeme oder Daten von ehemaligen Mitarbeitenden gibt, werden bei einem Ausscheidungsprozess Vorkehrungen getroffen. Die Ergebnisse der Befragung zeigen, dass je grösser ein Unternehmen ist, desto wahrscheinlicher liegt ein standardisierter IT-Ausscheidungsprozess. Im Schnitt haben Unternehmen mit bis zu zehn Mitarbeitern zu 48 % einen standardisierten Ausscheidungsprozess, wobei im Gegensatz 93 % der Grossunternehmen den Ausscheidungsprozess standardisiert ausführen.

Zusammenfassung

In Bezug auf den Stand der Praxis erlaubt unsere Umfrage folgende Rückschlüsse:

1. Viele der etablierten technischen Instrumente und Verfahren der Cyber-Sicherheit werden in Liechtensteiner Unternehmen weitgehend eingesetzt. Hierzu zählen vor allem Dokumentation der IT-Infrastruktur, regelmässiges Einspielen von Patches, rollenbasiertes Berechtigungsmanagement sowie Backup-Systeme.
2. Weniger, aber ausreichend verbreitet ist eine zentralisierte Verwaltung und Konfiguration von Endgeräten.
3. Ein deutliches Verbesserungspotenzial besteht bei der Definition von Disaster Recovery und Business Continuity Plans. Durch eine hohe Anzahl nicht angegebener Antworten auf diese Fragen lässt sich vermuten, dass einige Befragte diese Begriffe nicht kannten.
4. IT-Dienste werden zunehmend ausgelagert, darunter auch Cyber-Sicherheit. Unsere Ergebnisse zeigen, dass Sicherheitsdienste mit 44 % sogar deutlich häufiger extern betrieben sind als Datenverarbeitung (30 %).

Handlungsempfehlungen

Im letzten Kapitel stellen wir die Ergebnisse vor, die unmittelbar oder indirekt mit potentiellen Handlungsempfehlungen verbunden sind. Eine Übersicht der Ergebnisse ist in den folgenden Tabellen aufgeführt.

1 = Trifft gar nicht zu / 5 = Trifft voll zu	1	2	3	4	5	KA
Das Fürstentum Liechtenstein benötigt eine nationale Strategie zur Abwehr von Cyber-Angriffen.	8.3	13.8	20.2	20.2	33.9	3.7
Das Fürstentum Liechtenstein benötigt eine Anlaufstelle bei Fragen und Problemen zum Thema Cyber Sicherheit.	3.7	13.8	13.8	24.8	41.3	2.8
Mitarbeitende werden in regelmässigen Schulungen zu aktuellen Gefahren und Themen aufgeklärt.	19.3	19.3	17.4	19.3	20.2	4.6
Mitarbeitende mit Zugriff auf sensible Daten werden in regelmässigen Abständen im Umgang mit diesen geschult.	18.3	13.8	22.0	18.3	21.1	6.4

	Ja	Nein	KA
In Ihrem Unternehmen ist ein IT-Sicherheitsbeauftragter definiert.	69.7	24.8	5.5
Es existiert eine offizielle Informationssicherheitsrichtlinie bzw. ein IT-Sicherheitskonzept in Ihrem Unternehmen.	54.1	39.4	6.4
Die in Ihrem Unternehmen verwendeten Passwörter unterliegen einer Passwortrichtlinie.	66.1	29.4	4.6
Ihre Computersysteme schreiben Logs (Ereignisprotokolle) bezüglich der verschiedenen Zugriffe.	65.1	15.6	19.3
Mitarbeitende haben auf privaten Geräten (Smartphone, Laptop) Zugriff auf Firmeninformationen.	52.3	45.0	2.8
Der Zugriff auf kritische Systeme erfordert in Ihrem Unternehmen eine Zwei-Faktor-Authentifizierung.	37.6	42.2	20.2

Ihr Unternehmen verfügt über folgende Schutzmechanismen:	ja	nein
… Spam-Filter	92.7	7.3
… Phishing-Schutz	67.0	33.0
… Identitätsprüfung bei E-Mails	41.3	58.7
… Verschlüsselung / digitale Signatur bei E-Mails	35.8	64.2
… Beschränkungen bei der Verwendung des Internets (Zugriff auf Webseiten, Herunterladen von Dateien)	51.4	48.6
… Eine regelmässig überprüfte und gewartete Firewall	84.4	15.6
… Einen Proxyserver, um auf das Internet zuzugreifen	49.5	50.5

Wenn Sie in Ihrem Unternehmen alleine für das Thema Cyber Sicherheit verantwortlich wären, wie würden Sie ein vorhandenes Budget unter folgenden fünf Punkten aufteilen (prozentual):	
Organisatorische Sicherheitsmassnahmen	20.6
Mitarbeitertraining bezüglich Cyber-Sicherheit	18.5
Netzwerksicherheit	25.0
Datenarchivierung	19.8
Physische Sicherheit der IT-Infrastruktur	16.1

Analyse der Ergebnisse

Nationale Strategie und Anlaufstelle

Eine nationale Strategie zur Abwehr von Cyber-Angriffen dient als ein wesentliches Instrument für die Planung und Umsetzung von Massnahmen zur Minimierung der Risiken durch Cyber-Angriffe. Dabei hat eine nationale Strategie das Ziel, alle relevanten Faktoren im landesspezifischen Kontext zu identifizieren und deren Prioritäten und das Zusammenwirken abzuschätzen. Dadurch soll ein Leitfaden für die Regierung, die Wirtschaft und die Gesellschaft entstehen, nach dem die Massnahmen gegen Cyber-Angriffe kostenoptimiert umgesetzt werden können. Die meisten europäischen Länder haben solche Strategien verfasst und setzen sie aktiv um.

Die Teilnehmer dieser Umfrage wurden gebeten, die Notwendigkeit für die nationale Strategie zur Abwehr von Cyber-Angriffen in Liechtenstein auf der Skala von 1 (gering) bis 5 (sehr hoch) einzuschätzen. Dabei zeigte sich eindeutig, dass eine solche Strategie befürwortet wird. Mehr als die Hälfte der Befragten (53 %) stufte die Notwendigkeit mit hoch oder sehr hoch ein. Daraus lässt sich eine breite Unterstützung für die Entwicklung einer nationalen Strategie zur Abwehr von Cyber-Angriffen (die aktuell im Auftrag der Regierung des Fürstentums Liechtenstein erarbeitet wird) erkennen. Mehrere Länder bauen als ein Instrument zur Abwehr von Cyber-Angriffen nationale Anlaufstellen für die Behandlung von IT-sicherheitsrelevanten Fragen und Problemen auf. In Deutschland, zum Beispiel, agiert seit 2011 das Nationale Cyberabwehrzentrum (NCAZ) als zentrale Stelle für operative Zusammenarbeit diverser organisatorischer Einheiten mit Zuständigkeiten im Bereich der Informationssicherheit. In der Schweiz wird seit 2019 auf der Basis der 2004 gegründeten Melde- und Analysestelle Informationssicherung (MELANI) das nationale Zentrum für Cyber-Sicherheit mit umfassenden technischen und organisatorischen Kompetenzen aufgebaut, welches auch für die internationale Zusammenarbeit zu Fragen der Cyber-Sicherheit zuständig ist. In Liechtenstein existiert aktuell kein zentrales Organ für die Bearbeitung von Fragen und Problemen zum Thema Cyber-Sicherheit. Dessen Notwendigkeit wurde in dieser Umfrage klar bestätigt. Insgesamt 65 % der Befragten stufen die Notwendigkeit für eine zentrale Anlaufstelle mit hoch oder sehr hoch ein. Insbesondere kleinere oder mittlere Unternehmen befürworten (mit ca. 75 % positiver Rückmeldungen) den Aufbau einer solchen Stelle.

Im weiteren Verlauf dieses Kapitels analysieren wir Rückmeldungen zu wesentlichen organisatorischen und technischen Massnahmen der Cyber-Sicherheit, um den Handlungsbedarf bei der Umsetzung solcher Massnahmen zu ermitteln.

IT-Sicherheitsbeauftragter

Im Mittelpunkt der Schutzmassnahmen steht die Stelle eines IT-Sicherherheitsbeauftragten. Da heutige Cyber-Risiken ein erhebliches wirtschaftliches Risiko für Unternehmen darstellen, trägt die Unternehmensführung die Verantwortung für wesentliche Entscheidungen in Bezug auf die Abwehr von Cyber-Angriffen. Allerdings beinhalten solche Entscheidungen zum Teil komplexe technische Fragen, die nicht selten ausserhalb der Kompetenz der Geschäftsführung liegen. IT-Sicherheitsbeauftragte verbinden diverse Aspekte des Sicherheitsmanagements und unterstützen die Geschäftsleitung bei wesentlichen Entscheidungen in Bezug auf Cyber-Sicherheit. Alle anerkannten Standards zum IT-Sicherheitsmanagement sehen die Stelle eines IT-Sicherheitsbeauftragten als ein Kernelement des Managementprozesses.

Bezugnehmend auf die Ergebnisse unserer Umfrage kann festgestellt werden, dass Liechtensteiner Unternehmen sich der Schlüsselrolle eines Sicherheitsbeauftragten bewusst sind. Bei fast 74 % der befragten Unternehmen ist die Rolle eines IT-Sicherheitsbeauftragten definiert. Dabei ergibt sich eine klare Steigerung beim Anteil der positiven Antworten nach Unternehmensgrösse. Während von den kleinen Unternehmen mit weniger als 10 Mitarbeitenden «lediglich» 60 % einen IT-Sicherheitsbeauftragten ernannt haben, liegt dies bei grösseren Unternehmen mit mehr als 250 Mitarbeitenden bei beachtlichen 93 %.

IT-Sicherheitskonzept

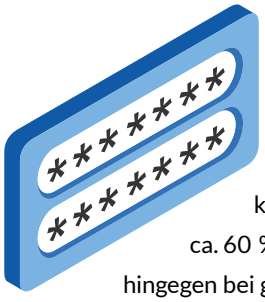
Eine Verbindung zwischen Geschäftsprozessen eines Unternehmens und den wesentlichen Aspekten des IT-Sicherheitsmanagements, insbesondere Sicherheitsrisiken und Sicherheitsmassnahmen, wird in einem IT-Sicherheitskonzept definiert. Durch die Verknüpfung von IT-Sicherheitsrisiken und Geschäftsprozessen können bei der Planung und Umsetzung von Massnahmen wesentliche Elemente der Geschäftsprozesse priorisiert werden. In der Regel wird ein IT-Sicherheitskonzept vom IT-Sicherheitsbeauftragten verfasst und dient als Leitfaden für weitere technische und organisatorische Entscheidungen.

Die Umfrageergebnisse zeigen, dass 58 % der Befragten über ein IT-Sicherheitskonzept verfügen. Bei dieser Frage ist ein klarer Unterschied zwischen den Unternehmen mit weniger als 50 Mitarbeitern (48 % der Befragten in dieser Kategorie haben ein Sicherheitskonzept erarbeitet) und Unternehmen mit mehr als 50 Mitarbeitern (über 80 % positive Antworten). Diese Ergebnisse belegen, dass das IT-Sicherheitsmanagement in Unternehmen von allen Grössen ernst genommen und in Abhängigkeit von verfügbaren Ressourcen systematisch geführt wird.

Passwörter und Protokolle

Eines der häufigsten Einfallstore für erfolgreiche Angriffe sind schwache Passwörter. Durch die gestiegenen Rechenkapazitäten wird es immer einfacher, schwache Passwörter durch so genannte «Brute-Force-Angriffe» zu knacken, auch wenn sie verschlüsselt gespeichert sind. Gelingt es dem Angreifer, ein Passwort für einen legitimen Benutzer zu erlangen, kann er damit alle Sicherheitskontrollen umgehen und die Rechte des betroffenen Benutzers geniessen. Oft erlauben diese lokalen Nutzerrechte die Gewinnung von privilegierten Rechten wie Administrator-Rechte (s. g. «privilege escalation»). Deswegen ist die Verwendung sicherer Passwörter eine der einfachsten und zugleich wirksamsten Schutzmassnahmen gegen Cyber-Angriffe. Eine Passwortrichtlinie informiert die Benutzer über die Anforderungen für Passwörter und legt die Prozesse und Massnahmen für die Wiederherstellung der vergessenen oder kompromittierten Passwörter fest.

Der Anteil von Unternehmen mit existierenden Passwortrichtlinien liegt laut Ergebnissen unserer Studie bei 70 %. Ähnlich wie beim IT-Sicherheitskonzept ist hier ein klarer Unterschied zwischen Unternehmen mit weniger bzw. mehr als 50 Mit-



arbeitenden zu erkennen. Bei kleineren Unternehmen verfügen ca. 60 % über eine Passwortrichtlinie, wohingegen bei grösseren Unternehmen der Anteil bei über 80 % liegt. Da die Passwortrichtlinie häufig als Teil eines IT-Sicherheitskonzepts definiert wird, ist die starke Korrelation zwischen den Antworten dieser beiden Fragen nachvollziehbar.

Protokollierung von Ereignissen in IT-Systemen ermöglicht eine bessere Erkennung und Aufklärung von Sicherheitsvorfällen. Die Erfahrung von prominenten Sicherheitsvorfällen zeigt, dass die Schadenshöhe sehr stark mit der Dauer bis zur Erkennung des Vorfalls korreliert. In heutigen IT-Systemen ist die Protokollierung von diversen Ereignissen bereits vorgesehen. Allerdings wird häufig von solchen Daten kaum Gebrauch gemacht, was in der Regel mit mangelnder Expertise oder fehlende personellen Ressourcen verbunden ist.

Etwa 65 % der Unternehmen gaben an, dass ihre Systeme über Ereignisprotokolle verfügen. Dieses Ergebnis spiegelt ein ausreichendes Sicherheitsbewusstsein bei Unternehmen wider. Auch hier ist eine klare Tendenz zu sehen, dass dieses Sicherheitsinstrument zunehmend häufig bei grösseren Unternehmen zum Einsatz kommt. Allerdings ist etwas beunruhigend, dass ca. 20 % der Befragten (vor allem bei kleineren und mittleren Unternehmen) keine Angabe machten. Dies zeigt, dass das Know-how für einige bereits existierende Werkzeuge nicht immer vorhanden ist.

Private Nutzung von Dienstgeräten

Viele Unternehmen gestatten ihren Mitarbeiterinnen und Mitarbeitern das Recht, ihre Arbeit auf privaten Geräten durchzuführen bzw. ihre dienstlichen Geräte für private Zwecke zu verwenden. Dies ermöglicht eine flexible Gestaltung der Arbeitszeiten und gilt als wichtige Massnahme, das Arbeitsklima attraktiver zu machen. Leider bringen beide Szenarien erhebliche Nachteile in Bezug auf die Sicherheit der verwendeten Geräte mit sich. Die private Nutzung findet grösstenteils ausserhalb der IT-Infrastruktur eines Unternehmens statt. Demzufolge können einige essentielle Sicherheitsinstrumente wie z. B. Firewall oder Webproxy nicht greifen. Bei der dienstlichen Verwendung von privaten Geräten kann ausserdem eine adäquate Wartung der Geräte nicht gewährleistet werden. Folglich sind private Geräte ein beliebtes Angriffsziel. Eine erfolgreiche Kompromittierung eines privaten Geräts ermöglicht einem Angreifer, die Identität des Opfers für weitere bösartige Zwecke zu missbrauchen. Eine vermeintliche E-Mail eines «Arbeitskollegen» kann andere Mitarbeiterinnen und Mitarbeiter dazu verleiten, infizierte Dokumente zu öffnen oder schadhaften Links zu folgen.

Die Verwendung von privaten Geräten im beruflichen Umfeld in Liechtenstein ist laut unserer Studie weit verbreitet. 52 % der Befragten bestätigten die Nutzung von privaten Geräten in ihren Unternehmen während 44 % dies nicht ermöglichen. Eine solche Verteilung weist an sich keine kritische Schwäche auf. Allerdings sollten aufgrund des erheblichen Grades der Nutzung von privaten Geräten entsprechende technische und organisatorische Massnahmen eingesetzt werden.

Mitarbeiterschulung

Sicherheitsvorfälle sind häufig unmittelbar mit einem menschlichen Fehler verbunden. Dazu zählen, wie bereits erwähnt, das Öffnen von infizierten Dokumenten oder das Verfolgen von schadhaften Links. Aber auch andere weniger bekannte Faktoren können zu Sicherheitsvorfällen führen. In öffentlichen WLAN-Netzen kann z. B. die Identität der Webseiten leichter gefälscht werden, daher sollten alle Internetdienste zwingend über sichere «Kanäle» wie z. B. VPN, TLS, SSH, o. Ä. abgewickelt werden. Auch alternative Verbindungstechnologien, z. B. Bluetooth, können für einen unerlaubten Zugriff auf interne Daten des Geräts missbraucht werden. Die Sensibilisierung von Mitarbeitenden zu aktuellen Gefährdungen kann die Risiken durch menschliche Fehler verringern und die Akzeptanz für technische und organisatorische Massnahmen steigern.

Unsere Befragung lässt keinen Rückschluss zur Ausführung von Schulungen für Mitarbeitenden erkennen. Die Verbreitung von solchen Schulungen wurde von Teilnehmenden unserer Umfrage auf

der Skala von 1 bis 5 geschätzt, wobei die Antworten gleich verteilt waren.

Authentifizierung

Der Zugriff auf sensible Daten erfordert besondere Schutzmassnahmen, die von Mitarbeitenden eingehalten werden müssen. Hierzu zählt, z. B. eine Zwei-Faktor-Authentifizierung, die Verwendung von virtuellen Desktops oder gar «Air-Gap»-Verfahren, bei denen der Träger physisch vom Rest des Systems getrennt wird. Die Sensibilisierung von Mitarbeitenden, die über einen Zugriff auf sensible Daten verfügen, ermöglicht einen routinierten und sicheren Umgang mit solchen Verfahren.

Ähnlich zur vorherigen Frage, lassen sich aus unseren Daten keine Tendenzen in Bezug auf die eingesetzten Schulungen erkennen, da die Antworten ebenfalls über die 5 verschiedenen Skala-Werten gleich verteilt sind.

Aufgrund der steigenden Risiken von passwortbasierter Authentifizierung werden heute zunehmend Zwei-Faktor-Authentifizierungsverfahren eingesetzt, welche die Offenlegung von zwei unabhängigen Merkmalen erfordern, um die Zugriffsberechtigung nachzuweisen. Neben dem passwortgeschützten Zugriff, welcher als üblicher Faktor gilt, werden dabei biometrische Merkmale, z. B. Fingerabdruck oder weitere geheime Informationen herangezogen, beispielsweise der Besitz eines speziellen Geräts / App.

Die Tendenz zur Verwendung der Zwei-Faktor-Authentifizierung für den Zugriff auf kritische Systeme fällt eher negativ aus. 42 % der Befragten berichten über keinen Einsatz von Zwei-Faktor-Authentifizierung während etwa 37 % positiv antworteten. Auffällig ist, dass 20 % der Teilnehmer die Frage nicht beantworteten, was eher als eine negative Antwort interpretiert werden kann.

Die Wahl von technischen Schutzmechanismen hängt von der konkreten Sicherheitsstrategie jedes einzelnen Unternehmens ab. Diese Wahl ist von vielen Faktoren beeinflusst: dem Aufwand, den Kosten, den vertretbaren Einschränkungen für Geschäftsprozesse, der Benutzerfreundlichkeit, usw. Die in der Umfrage gestellten Fragen messen den Verbreitungsgrad von gängigen technischen Schutzmechanismen, insbesondere dem Schutz von E-Mail-, Netz- und Internetverkehr.

Die Ergebnisse zeigen, dass die meisten Unternehmen relativ gut gegen Angriffe via E-Mail aufgestellt sind. 92 % der Befragten benutzen Spamfilter und 67 % der Befragten setzen Schutzmassnahmen gegen Phishing ein. Auch die Netzwerke der teilnehmenden Unternehmen sind durch konfigurierte und gewartete Firewalls in der Regel gut geschützt (84 %). Weniger verbreitet ist der kontrollierte Zugriff auf das Internet. Nur etwa die Hälfte der Befragten setzt solche Kontrollen entweder organisatorisch durch die Zugriffsregeln oder technisch durch den Einsatz eines Webproxyserves um. Noch weniger verbreitet sind Schutzmechanismen für die Integrität und Vertraulichkeit von E-Mail. Nur etwa 41 % der Befragten setzen Identitätsprüfung beim Versand von E-Mails um, und lediglich 35 % verwenden Verschlüsselung und digitale Signaturen.

Die spezifische Gestaltung von Schutzmassnahmen gegen Cyber-Angriffe hängt massgeblich von den wirtschaftlichen Ressourcen und spezifischen Gegebenheiten der Geschäftsprozesse eines Unternehmens ab. Die Investition in die IT-Sicherheit zahlt sich nur dann aus, wenn sich dadurch konkrete wirtschaftliche Risiken minimieren und entsprechend «Gewinne» erzielen lassen. Um mögliche Schwerpunkte für Investitionen in Cyber-Sicherheit zu erkunden, wurden die Teilnehmenden gebeten, ihr hypothetisches Budget für Cyber-Sicherheit auf 5 Bereiche zu verteilen. Als wichtigster Bereich ergab sich daraus Netzsicherheit, mit ca. 25 % des Gesamtbudgets. Es folgten organisatorische Massnahmen (22 %), Datenarchivierung (19 %), Mitarbeitertraining (18 %) und physische Sicherheit (16 %). Eine relativ gleiche Verteilung des Budgets zeigt, dass die Komplexität der Aufgabe sowie die daraus resultierende Notwendigkeit von verschiedenen Mechanismen generell gut wahrgenommen sind.

Zusammenfassung

Folgende Handlungsempfehlungen ergeben sich aus unserer Studie:

1. Liechtenstein braucht eine Strategie zum Schutz gegen Cyber-Risiken sowie eine Anlaufstelle für Fragen bei Problemen auf dem Gebiet der Cyber-Sicherheit. Beide Massnahmen wurden von einer deutlichen Mehrheit der Befragten befürwortet.
2. Unternehmen sollen der Mitarbeiterschulung in Bezug auf Cyber-Sicherheit deutlich mehr Aufmerksamkeit zukommen lassen.
3. Aufgrund der stark verbreiteten Nutzung von privaten Geräten in den Unternehmen (über 50 % der befragten Unternehmen) ist der Einsatz von speziellen Lösungen für die sichere Integration in die IT-Infrastruktur zu empfehlen.
4. Aufgrund eines zunehmenden Risikos passwort-basierter Authentifizierung ist der Ausbau von Zwei-Faktor-Authentifizierung für Zugriff auf kritische Daten / Systeme zu empfehlen. Aktuell ist der Verbreitungsgrad dieser Techniken mit ca. 38 % eindeutig zu gering.
5. Die Verwendung von Schutzmechanismen für E-Mails (Verschlüsselung und digitale Signaturen) soll ausgebaut werden. Hierzu soll eine Infrastruktur für die sichere Identifikation und Generierung von digitalen Signaturen aufgebaut und den Unternehmen zur Verfügung gestellt werden.

Schlussbemerkungen

Die durchgeführte Studie zeigt, dass das Thema Cyber-Sicherheit in Liechtensteiner Unternehmen gut verankert ist. Auch wenn die vorhandene Fachexpertise generell als unzureichend empfunden wird, ist klar, dass aus organisatorischer Sicht die erforderlichen Aufgaben sehr ernst wahrgenommen werden. Die meisten der befragten Unternehmen setzen die als Standard geltenden Massnahmen konsequent um, insbesondere in Anbetracht der vorhandenen finanziellen und personellen Ressourcen. So ist selbst bei kleineren Unternehmen bei der Umsetzung von Massnahmen, wie Erarbeitung eines Sicherheitskonzepts, Dokumentation der IT-Infrastruktur, Aktualisierung von Software, zentralisierte Verwaltung von Zugriffsberechtigungen, eine verhältnismässig hohe Quote von 60-70 % zu erkennen. Auch bei technischen Massnahmen werden viele gängige Technologien eingesetzt, wie Spam- und Phishing-Schutz, Backups und Firewalls. Diese Erkenntnisse belegen einen adäquaten und ressourcenbewussten Schutz vor üblichen Sicherheitsbedrohungen. Auch sehr lobenswert ist die Tatsache, dass über 75 % der Unternehmen sich in den nächsten zwei Jahren vermehrt mit der Verbesserung der Cyber-Sicherheit beschäftigen werden.

Mit dem Blick in die Zukunft zeichnen sich allerdings auch einige Herausforderungen ab, die vor allem kleine und mittlere Unternehmen betreffen. Besonders auffällig ist, dass viele dieser Unternehmen das Cyber-Risiko für sich selbst als tendenziell gering einschätzen. Demzufolge zeigen sich bei der Analyse der Verwendung aktueller Sicherheitsinstrumente mehrere Aspekte, bei denen kleinere Unternehmen einen deutlichen Nachholbedarf haben. Dies betrifft z. B. die automatisierte Verwaltung von Endgeräten sowie Ausarbeitung von Disaster Recovery und Business Continuity Plans.

Als wichtigste Handlungsempfehlungen ergeben sich die Erarbeitung einer nationalen Strategie zum Schutz vor Cyber-Risiken sowie die Ausarbeitung einer Kontaktstelle für Fragen und Problemstellungen in der Cyber-Sicherheit. Diese beiden Instrumente sollen den Nutzungsgrad von üblichen Schutztechnologien und Methoden deutlich erhöhen und somit das Sicherheitsniveau für eine breitere Schicht der Unternehmen - unabhängig von dessen Grösse - auf einen hohen Standard bringen. Eine weitere wichtige Aufgabe ist die Intensivierung Intensivierung des Austauschs von Informationen und Fachwissen in Liechtenstein. Diese sollen insbesondere alle Unternehmen über aktuelle Cyber-Risiken aufklären und bei Bedarf Wissen an deren Mitarbeiterinnen und Mitarbeiter weitergeben.

Auf der technischen Seite ergeben sich auch einige Aspekte, die eine wichtige Rolle in der Zukunft spielen werden. Mit steigendem Einsatz von privaten Geräten im beruflichen Umfeld werden entsprechende neue Sicherheitstechnologien erforderlich, um die daraus resultierenden Risiken zu minimieren. Eine weitere wichtige technologische Entwicklung ist der Einsatz von Zwei-Faktor-Authentifizierungsverfahren für den Zugriff auf kritische Daten. Diese Technologien können auch dazu beitragen, die Sicherheit von E-Mail-Kommunikation durch den flächendeckenden Einsatz von Ende-zu-Ende-Verschlüsselung und Integritätsschutz zu erhöhen. Hierzu ist der Aufbau der Infrastruktur für eine sichere Identifikation und Generierung von digitalen Signaturen notwendig.

Weiterführende Informationen und Download der Studie finden Sie auf: **www.digital-liechtenstein.li**

digital-liechtenstein.li

Träger

REGIERUNG
DES FÜRSTENTUMS LIECHTENSTEIN

Patronat

S. D. Erbprinz
Alois von und zu
Liechtenstein

Partner

CYBERCHECK.LI

Testen Sie jetzt kostenlos und anonym die Sicherheit Ihres Unternehmens!

Für den Digitalstandort Liechtenstein hat IT-Sicherheit oberste Priorität – der kostenlose Schnellcheck auf **www.cybercheck.li** erlaubt Ihnen eine erste Einschätzung des Schutzes vor Cyber-Attacken. Er berücksichtigt organisatorische, technische und physische Massnahmen und liefert im Ergebnis konkrete Empfehlungen zur Verbesserung Ihrer IT-Sicherheit.

www.cybercheck.li

Hier gehts zur Website

Fachbeiträge **Videointerviews** **Beratungsstellen**

Eine Kampagne von digital-liechtenstein.li

Hauptpartner

Partner