

Digital-liechtenstein.li präsentiert Studie zu Cybersicherheit

Hohes Risiko für den Wirtschaftsstandort: Jedes zweite Unternehmen in Liechtenstein ist bereits Opfer eines Cyberangriffs geworden.

Eine neue Studie der Universität Liechtenstein im Auftrag von Digital-liechtenstein.li zeigt die Schwachstellen deutlich auf. Cybersicherheit gilt als unerlässliche Voraussetzung für den Erfolg der digitalen Transformation. Dies betrifft sowohl Grossunternehmen als auch KMU. Die Standortinitiative Digital-liechtenstein.li hat nun eine Studie in Auftrag gegeben, um die aktuelle Lage der Cybersicherheit für den Wirtschaftsstandort Liechtenstein einzuschätzen.

Die Studie wurde unter der Federführung von Professor Pavel Laskov, Inhaber des Hilti-Lehrstuhls für Daten- und Anwendungssicherheit an der Universität Liechtenstein, gemeinsam mit Studierenden erarbeitet und basiert auf einer repräsentativen Umfrage bei über 100 Unternehmen sowie verschiedenen Verwaltungsstellen in Liechtenstein.

Hohe Trefferquote bei Cyberangriffen

Die Resultate sind eindeutig: Eine grosse Mehrheit der Befragten sieht ein hohes Risiko für Unternehmen in Liechtenstein, Opfer eines Cyberangriffs zu werden. Diese Erkenntnis wird auch von den Statistiken zu Sicherheitsvorfällen belegt. Jedes zweite Unternehmen berichtete über Sicherheitsvorfälle, bei grossen Unternehmen liegt die Trefferquote gar bei 100 Prozent. Nachdem die Umfrage nur bekannte Vorfälle erfassen kann und die Dunkelziffer hoch ist, ist die tatsächliche Anzahl der betroffenen Unternehmen womöglich deutlich höher. Unterschiede zeigen sich in der Risikowahrnehmung nach der Grösse des Unternehmens. Je kleiner das Unternehmen, desto geringer ist die Einschätzung des eigenen Sicherheitsrisikos, was laut den Studienautoren eine gefährliche Entwicklung ist.

Liechtensteiner Unternehmen sind jedenfalls nicht tatenlos. Entscheidend für eine erfolgreiche Abwehr der Cyberangriffe ist nicht immer umfassendes technisches Know-how. Vielmehr zählen dazu grundsätzliche Vorkehrungen wie die Erarbeitung eines Sicherheitskonzepts, die Benennung eines Sicherheitsbeauftragten, die adäquate, rollenbasierte Zugriffskontrolle sowie der Einsatz von gängigen technischen Instrumenten wie Datensicherung, Firewalls und Phishing-Schutz. Wie die Studie zeigt, sind diese Massnahmen



Vertreter von Digital-liechtenstein.li diskutierten die Ergebnisse der Studie vor Kurzem auf Schloss Vaduz mit Erbprinzen Alois von und zu Liechtenstein.

Bild: zvg

bei einem hohen Anteil der befragten Unternehmen bereits umgesetzt. Die Studie geht auf weitere zentrale Faktoren ein, auch auf das aktuelle Thema der Verschmelzung von Arbeitswelt und Privatleben, wodurch private Geräte immer häufiger auch im beruflichen Umfeld eingesetzt werden.

Private Geräte bergen Sicherheitsrisiken

Bereits heute berichtet rund die Hälfte der befragten Unternehmen, dass sie eine Nutzung privater Geräte zulassen. «Gerade im Zusammenhang mit der Covid-19-Pandemie haben wir einmal mehr die Verwundbarkeit der digitalen Welt gesehen, seien es Angriffe gegen Videokonferenzsysteme, tagesaktuelle Phishing-Angriffe oder Fake-Pharmacy-Sites.

Die eindeutigen Vorteile der Digitalisierung gibt es nicht ohne entsprechende Sicherheitskonzepte», sagt Professor Jan vom Brocke, Leiter des Instituts für Wirtschaftsinformatik. Dem Stellenwert von Sicherheitskonzepten sollte daher in Zukunft deutlich mehr Aufmerksamkeit geschenkt werden. Als weitere wesentliche Baustelle

wird die Verwendung von Zwei-Faktor-Authentifizierung genannt. Aktuell setzen weniger als 40 Prozent der Unternehmen diese grundlegende Massnahme für den Zugriff auf sensitive Daten um. Angesichts der steigenden Risiken durch verwendete Passwörter ist dieser Wert laut der Studie eindeutig zu gering.

Empfohlen wird daher der stärkere Einbezug von Expertenempfehlungen. Outsourcing – beispielsweise von IT-Sicherheitsdiensten – würden aktuell am häufigsten die mittleren Unternehmen nutzen, wobei insbesondere Kleinstunternehmen – ein finanziell tragbares Angebot vorausgesetzt – davon zweifellos noch mehr profitieren können.

Neue Rolle? Staat ist gefragter denn je

Auch der Staat kann einen wichtigen Beitrag zur Förderung der Cybersicherheit in Liechtenstein leisten. Über 70 Prozent der Befragten befürworten die Ausarbeitung einer nationalen Strategie zur Abwehr von Cyberangriffen sowie den Aufbau einer Anlaufstelle für Fragen und Probleme

zum Thema Cybersicherheit. Diese beiden Massnahmen würden eine Weiterentwicklung von Fachkompetenzen in der Cybersicherheit spürbar beschleunigen. Auch Aus- und Weiterbildungen sind gefragt, denn die Nachfrage an Fachkompetenzen wird deutlich steigen. 75 Prozent der Unternehmen geben an, sich in den kommenden zwei Jahren aktiv mit dem Ausbau der Cybersicherheit zu beschäftigen.

Die Beteiligten konnten die Ergebnisse der Studie kürzlich gemeinsam mit Erbprinzen Alois von und zu Liechtenstein diskutieren. Lothar Ritter, Boardpräsident 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 zentrale Herausforderung für Liechtenstein: «Die Pandemie hat in Bereichen wie Homeoffice und Homeschooling die grosse Be-

deutung einer stabilen und sicheren Dateninfrastruktur für unsere heutige Gesellschaft gezeigt. Staat und Wirtschaft sollten daher beim Thema Cyber Security eine enge Zusammenarbeit sicherstellen.»

Kampagne «Cyber Security Liechtenstein»

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 Cybersicherheit 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 Empfehlungen machen und das finanzielle Risiko eines Cyberangriffs kalkulieren können. Auch hat die Initiative bereits verschiedene Workshops und Veranstaltungen durchgeführt. Spezielle Partner der Kampagne sind die Funk-Gruppe, Funk Stiftung, FL1, die Universität Liechtenstein, BDO, MTF Group, Speedcom und HSL Informatik. (pd)

Noch kein Vaterland-Abo?

- ✓ Unbeschränkter Zugriff auf vaterland.li
- ✓ E-Paper: Liewo, KuL, «Vaterland»-Magazine
- ✓ Vaterland-News per SMS
- ✓ E-Paper «Liechtensteiner Vaterland» – Montag bis Samstag täglich ab 24 Uhr in der App news.li und online auf vaterland.li verfügbar
- ✓ unbeschränkter Zugang zum Online-Archiv seit 1914
- ✓ Jeden Freitag: Wirtschaft regional E-Paper

nur
CHF **69.-**
Aktionsabo
für 3 Monate
Print + E-Paper



E-Paper Hotline:
Telefon
+423 236 16 61
E-mail
abo@vaterland.li

Jetzt bestellen – ab sofort nichts mehr verpassen! Abo bestellen: +423 236 16 61, abo@vaterland.li