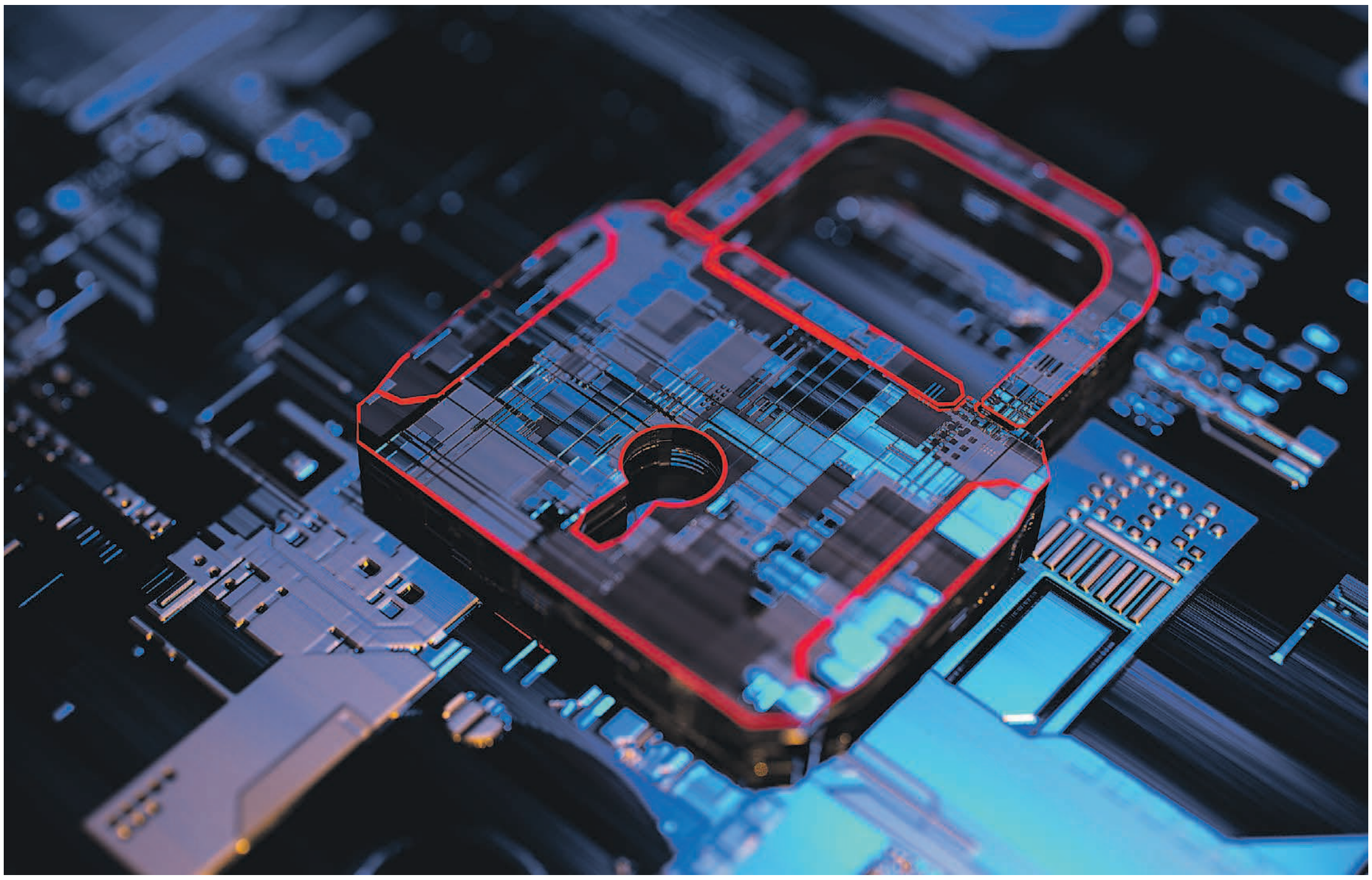

# Schutz vor der digitalen Schattenseite

Während sich ein grosses Unternehmen wie die LLB dank interner Spezialisten und ausgeklügelter technischer Lösungen effektiv gegen Cyberkriminalität wehren kann, weisen KMUs teilweise erheblichen Nachholbedarf auf.

OLIVER BECK

Wie jede Medaille hat auch diese zwei Seiten: Die fortschreitende Digitalisierung birgt nicht nur viele Chancen, sondern gleichermassen Risiken und Gefahren. Attacken auf Daten und technische Infrastrukturen schweben als mögliches Szenario, einer dunklen Wolke gleich, über der durch und durch vernetzten Welt. Gänzlich sicher, das zeigen die wiederkehrenden Angriffe aus dem Cyber-Hinterhalt, ist niemand – nirgendwo und niemals. Die Liechtensteinische Landesverwaltung etwa hat das erst Ende September wieder vor Augen geführt bekommen. Über vermeintlich von ihr versandte E-Mails hatten Betrüger versucht, einen E-Banking-Trojaner auf den Rechnern der Empfänger einzuschleusen. Allein innerhalb der Landesverwaltung gingen die sogenannten Phishing-E-Mails an gut 50 Personen. Die Zahl der externen Betroffenen konnte nicht eruiert werden.

## Kaspersky: Oft fehlt der Plan

Nur wenige Tage später hob Eugene Kaspersky, Gründer und Chef des gleichnamigen Antiviren-Softwareunternehmens, anlässlich der Eröffnung der Münchner Cyber-Security-Messe «Command Control» mahnend den Finger. «Viele verstehen immer noch nicht, was sie tun müssen», sagte er und meinte damit vor allem die Unternehmen und ihre Vorkehrungen, um sich respektive ihre Kunden bestmöglich vor Angriffen zu schützen. Gefahr erkannt, aber unzureichend gebannt. Eine Einschätzung, in der sich die Liechtensteiner Akteure womöglich ein Stück weit selbst wiedererkennen?

«Nein», antwortet Martin Kast, Leiter Group Information Security der LLB-Gruppe, bestimmt. «Die Bedrohungsszenarien im digitalen Zeitalter sind vielfältig und stellen grosse Herausforderungen für die Unternehmen dar. Über die möglichen Folgen der digitalen Vernetzung nachzudenken, Sicherheitsvorkehrungen zu überprüfen und Angriffspunkte systematisch abzusichern, ist für die LLB das Gebot der Stunde.» Die Bemühungen des Finanzinstituts fokussieren dabei verschiedene Ebenen. Im Bereich der Technik setzt es beispielsweise auf eine entsprechend konzipierte Software-Architektur. «Mittels eigenständiger Systeme trennen wir strikt öffentliche und persönliche Daten», erläutert Kast. Ebenso habe man für den Zahlungsverkehr ein breit angelegtes, selbstlernendes Fraud-Detection-System entwickelt.

## IT-Spezialisten im Haus

Eine andere, damit korrespondierende Massnahme besteht in der Beschäftigung von Spezialisten. Die Abteilung Group Information Security erstelle, implementiere und pflege das Informationssicherheitsprogramm nach unternehmensweit gültigen Weisungen, sagt deren Leiter. Die Group IT wiederum kümmere sich um die technische Umsetzung und das Sicherheits-Monitoring. Parallel dazu analysieren die Fachstellen «kontinuierlich die neuen Risiken, die sich aus Cyberbedrohungen ergeben und ergreifen die jeweils passenden Abwehrmassnahmen», so Kast.

Schliesslich gehört zu den zentralen Sicherheitsvorkehrungen der LLB auch die Sensibilisierung ihrer Mitarbeiter. Neben fortwährenden Schulungen speziell für neue Kräfte fanden und finden 2018 laut Kast auch Wiederauffrischungs-Kurse für 400 Mitarbeiter statt, die seit mehr als vier Jahren für die LLB-Gruppe tätig sind. Seit 2017 verfolgt das Unternehmen zudem den Ansatz, seinen Mitarbeitenden das Thema Cyber Security mittels Smartphone-Lernspiel näherzubringen. «Durch das IT-Security-Training lernen auch weniger technikaffine Mitarbeitende auf spielerische Art den Umgang mit Themen wie ‹Phishing›, ‹DDos-Attacken› oder ‹Social Engineering›.»

Der Massnahmenkatalog hat sich in der Praxis bereits bei verschiedenen Gelegenheiten bewähren können, wie Kast sagt. Im November 2015 wie auch im August 2018 hätten etwa Phishing-Versuche erfolgreich vereitelt werden können. «Dank unserer Sicherheitsvorkehrungen und der schnellen Reaktion der Nutzer kamen keine Kunden zu Schaden.»

Auch genügend kleinere Liechtensteiner Unternehmen haben mit Cyber-Kriminalität ihre unliebsamen Erfahrungen gemacht, berichtet Wirtschaftskammer-Geschäftsführer Jürgen Nigg. «Der Klassiker sind sicherlich E-Mails im Namen des Inhabers, die intern in die Buchhaltung gehen und in denen eine dringende Auslandsüberweisung gefordert wird», erzählt er. Weil die übermittelten Nachrichten teils täuschend echt seien, sei die Gefahr gross, dass ein Mitarbeiter auch tatsächlich eine Überweisung vornehme.

## Risiko noch immer unterschätzt

Im Wissen um die ständig lauernde Gefahr versucht der Dachverband für Gewerbe, Handel und Dienstleistungen seinen Beitrag zur Prävention zu leisten. «Die Wirtschaftskammer sensibilisiert ihre Mitglieder auf verschiedenen Kanälen, sei dies mit Infoveranstaltungen durch die Sektion ProIT oder mit gezielten Schulungen bei kurse.li», so Nigg. Auch das diesjährige Unternehmerforum habe sich der Themen Digitalisierung und Gefahr durch Cyber-Attacken ausführlich angenommen.

Und doch hinkt die Bewusstseinsbildung in zahlreichen Liechtensteiner KMUs der Realität noch immer merklich hinterher, sagt Harald Rüdisser, Pressebeauftragter des IT-Unternehmens SpeedCom: «Das Risiko eines Cyber-Angriffs hat sich in den letzten Jahren stetig erhöht und wird in der Praxis leider viel zu oft unterschätzt.» Entsprechend sei das Modell, dass ein Betrieb die IT-Systeme selbst verwalte oder einen Kollegen mit ‹IT-Kenntnissen› mit dieser Aufgabe betraue, noch immer weit verbreitet. «Dies führt über kurz oder lang zu Sicherheitslücken, die fatale Folgen haben können.»

## Schwachstelle Mensch

Deutlich besser fährt ein KMU angesichts immer komplexer werdender Anforderungen, wenn es die Verantwortung für den Schutz von Daten und technischer Infrastruktur in die Hände eines professionellen IT-Partners legt. «Die KMU verlassen sich dann ganz auf die Empfehlungen des IT-Partners – dieser trifft die technischen notwendigen Massnahmen in den Bereichen Firewall, E-Mail-Security und Antivirus», schildert Rüdisser, dessen Unternehmen selbst mehrere kleinere Betriebe im Mandat betreut. Doch damit allein ist es nicht getan, betont er: «Ein weiterer wichtiger Punkt ist die Sensibilisierung der Mitarbeiter – denn Cyberkriminelle fokussieren sich immer stärker auf das menschliche Fehlverhalten.» Gerade in dieser Hinsicht sei bislang noch zu wenig passiert.

## Sensibilisierung kann viel bewirken

Dass sich Unternehmen und Behörden gut gegen Cyber-Attacken zu wappnen wissen, ist der nationalen Datenschutzstelle (DSS) naturgemäss ein wichtiges Anliegen. Entsprechend informiert sie im Rahmen von Veranstaltungen regelmässig über aktuelle Entwicklungen im Bereich der Datensicherheit und hat auch schon eine sich gerade in Überarbeitung befindliche Empfehlung zu technischen und organisatorischen Massnahmen veröffentlicht, wie Michael Valersi sagt. Besonders bedeutsam, fährt der stellvertretende DSS-Leiter fort, sei aber auch «der regelmässige Austausch mit den Sicherheitsverantwortlichen sowohl von Behörden als auch von privaten Unternehmen». Ein Dialog, den die Datenschutzstelle aktiv pflege.

Als erste Massnahme für mehr Datenschutz und Datensicherheit empfiehlt die Datenschutzstelle die interne Sensibilisierung. «Aufmerksame Mitarbeiter», betont Michael Valersi, «können das Sicherheitsniveau signifikant verbessern, ohne dass grosse technische Investitionen getätigt werden müssen, die zudem häufig nicht das leisten können, was sich die Verantwortlichen erwarten.» *(bo)*