Neue Cyber Security Allianz

Mit der neugegründeten Allianz für Cyber-Sicherheit verfolgen die Firmen BDO, Funk Gruppe und Telecom Liechtenstein das Ziel, die Widerstandsfähigkeit des Standortes Liechtenstein gegenüber Cyber-Angriffen zu stärken. IT-Dienstleistungs- und -Beratungsunternehmen sowie IT-Hersteller sind gleichermassen im Netzwerk vertreten wie Anwenderunternehmen aller Grössen und Branchen. Diese Vielfalt ist ein wichtiger Garant für einen reichhaltigen Austausch von IT-Expertise und Anwendungserfahrungen, von dem alle Beteiligten profitieren.

Wie ist es zu diesem Zusammenschluss gekommen?
Aldo Frick (Telecom Liechtenstein): Die 3 Firmen BDO, FUNK und Telecom Liechtenstein bieten eigenständig unter anderem Dienstleistungen rund um das Thema Cyber Security an Geschäftskunden im Fürstentum Liechtenstein an.
In mehreren vorangegangenen Gesprächen und durch Kundenfeedbacks hat sich gezeigt, dass das selbe Segment bearbeitet wird und in den angebotenen Leistungen keine Überschneidungen zu erkennen sind. Vielmehr werden Leistungen angeboten, die komplementär zueinanderstehen und sich gegenseitig für den Kunden nutzenstiftend ergänzen.
Der Cyber Security Lunch 2019 war bereits ein voller Erfolg. Corona-bedingt etwas verspätet findet nun der Event 2020 im November statt. Unternehmerinnen und Unternehmer können sich über die Mittagszeit ein Bild machen, was sich in der Cyber Security Praxis bewährt hat und wie das Thema im eignen Unternehmen angegangen werden kann.

Gibt es mehr Angriffe auf Firmen im Vergleich zu früher?
Andy Bircher (FUNK): Die Zahlen sprechen eine deutliche Sprache. Internationale Studien zeigen, dass sich die Angriffe in den letzten Jahren dynamisch entwickelt haben. Dabei ist festzuhalten, dass nicht nur die Anzahl der Angriffe auf jedes Unternehmenssegment stark zugenommen hat, sondern auch die Qualität der Angriffe eine hohe Professionalität aufweisen.

Die im Frühjahr 2020 im Rahmen der Digital Roadmap erarbeitete Studie der Universität Liechtenstein «Cyber-Sicherheit in Liechtenstein» hat u. a. folgende Resultate gezeigt: Über 60% der mittelständischen Unternehmen in Liechtenstein rechnen tendenziell damit, Opfer eines Cyberangriffes zu werden. 70% der Unternehmen würden bei einem erfolgreichen Angriff massgeblich in ihrer Leistungserbringung behindert. Der Corona-beschleunigte Trend zum Home-Office hat nun die Verwundbarkeit der Unternehmen noch zusätzlich erhöht. Das wird von Cyber-Kriminellen skrupellos ausgenutzt.

Das Thema Cyber Security ist sehr präsent, was muss eine Firma machen um sich vor Angriffen zu schützen?
Christian Wolf (BDO): Das hängt natürlich sehr von der Branche und vom Geschäftsmodell der Firma ab. Zentral ist für alle Unternehmen, dass Mitarbeitende und Geschäftsleitung regelmässig zu Cybergefahren, IT-Sicherheit und Datenschutz trainiert werden. Selbstverständlich muss auch das technische Abwehrdispositiv regelmässig überprüft und der neuen Bedrohungssituation angepasst werden. Früher hat haben viele Unternehmen das Thema an die IT-Abteilung delegiert. Cybersicherheit ist heute jedoch klar ein Thema auf Stufe Geschäftsleitung und Verwaltungsrat

Welche Aspekte umfasst die IT Sicherheit abseits der technischen Lösungen?
Christian Wolf (BDO): Die IT-Sicherheit umfasst für uns die drei Säulen «organisatorische Sicherheit», «physische Sicherheit» und die «technische Sicherheit». Dabei steht die organisatorische Sicherheit bewusst am Anfang, weil der «Faktor Mensch» vielfach das grösste Gefahrenpotential darstellt. Aus unserer Sicht wird heute noch zu viel in technische Lösungen investiert und zu wenig in die Schulung der Mitarbeiter, um deren Bewusstsein hinsichtlich Cyber-Gefahren zu schärfen. Denn der Mitarbeiter selbst wird immer häufiger als «vermeintliche Sicherheitslücke» für Cyber-Angriffe ausgewählt.

Was für technische Möglichkeiten gibt es um einen Basisschutz zu erlangen?
Aldo Frick (Telecom Liechtenstein): Die Breite und Tiefe der Lösungen ist sehr gross. Ein absolutes Minimum an Schutz bieten Antiviren und Firewall Lösungen, welche heute zum Standard gehören. Leider hört hier bei vielen Unternehmen bereits ihr Basisschutz auf. Aus meiner Sicht ist ein Offline Backup, am besten

Aldo Frick CEO FL1, Christian Wolf Partner BDO, Andy Bircher CEO Funk Gruppe Liechtenstein (Foto: ZVG)

ausserhalb des Hauptsitzes ebenfalls unabdingbar. Damit der Basisschutz wirksam bleibt, müssen die Systeme mit den aktuellen Security Updates aktuell gehalten werden. Angreifer entwickeln ihre Techniken stetig weiter und mit dieser Entwicklung muss man schritthalten können. Ist ein Angreifer dann doch einmal erfolgreich, so hilft es, wenn er ein gut segmentiertes Netzwerk vorfindet, in dem alle Services mit den geringsten möglichen Berechtigungen bereitgestellt wurden. Endpoint Detection & Response Systeme helfen bei der Erkennung solcher Angriffe und können ein wichtiges Tool sein, um die Eindringlinge wieder vor die Türe zu setzen. Wir empfehlen Ihre technischen Sicherheitsmassnahmen von Experten beurteilen zu lassen und regelmässige Schwachstellenscans durchzuführen.

Wie schützt man sich vor finanziellen Folgen eines Cyberangriffs?
Andy Bircher (FUNK): Vorerst geht es darum zu verstehen, was in einem Cyber-Worst-Case finanziell auf dem Spiel steht. Es liegt auf der Hand, dass die diesbezügliche Analyse sehr kundenspezifisch ist. Auf Cyber-Check.li können Unternehmen mit dem Funk Cyber Risk Calculator eine grobe Berechnung anstellen, was der finanzielle Cyber-Worst-Case für sie bedeuten würde. Eine Detailberechnung mit entsprechender Diskussion im Management (Cyber Risiko Dialog) führt erfahrungsgemäss zu den besten Resultaten. Die Herleitung des finanziellen Risikos wird so auch für den Verwaltungsrat eines Unternehmens nachvollziehbar. Anschliessend geht es darum abzuwägen, ob das Risiko durch das Unternehmen getragen werden kann oder ob eine Cyberversicherung sinnvoll ist. Unternehmen mit einer guten Cyberfitness finden im Markt auch eine gute Versicherungsdeckung. Die diesbezüglichen Anforderungen an die Unternehmen steigen stetig und auch die Preise für Cyberversicherungen haben in den letzten Monaten deutliche Erhöhungen erfahren.

Was erwarten die Besucher am Cyber Security Lunch?
Christian Wolf (BDO): Gut dargestellte Beispiele aus dem Markt Liechtenstein anhand echter Cases. Konkrete Lösungsansätze, die als Anregung diesen sollen. Netzwerken mit der Branche, andere Unternehmen, Experten und den führenden Anbietern am Markt. (pr)

Anmeldungen unter Xing Events oder unter www.cyberalliance.li

CYBER SECURITY LUNCH, 5. NOVEMBER 2020, SAL, SCHAAN

Programm

10.00 Uhr Eintreffen der Gäste/Registration
10.30 Uhr Beginn und Begrüssung, Rob Hartmans, Moderation
10.40 Uhr Cyber-Security in der Praxis, Manuel Pfiffner, IT-Manager und Christian Wolf, Partner, BDO Liechtenstein AG
11.00 Uhr Cyber-Abwehrkräfte technisch stärken, Aldo Frick, CEO, und Christoph Malin, Senior Expert Cyber Security, Telecom Liechtenstein AG
11.20 Uhr «Cyber-Fitness» für Ihr Team, Andy Bircher und Rolf Th. Jufer, Geschäftsleitung, Funk Gruppe Liechtenstein
11.40 Uhr Podiumsdiskussion
12.10 Uhr Lunch