IT-Experte Fridel Rickenbacher zum Thema Cyber-Security

Den Schlusspunkt der Generalversammlung des Gewerbevereins Schwyz setzte Marco Zörner mit einem spannenden Interview mit IT-Experte Fridel Rickenbacher zum Thema Cyber-Security.

Wie steht es um die (Cyber-) Sicherheit der KMU in der Schweiz?

«Es sind unterschiedliche Ausprägungen anzutreffen, zwischen unbewusster Inkompetenz und entsprechend falschem Vertrauen in eine vermeintliche Sicherheit bis zur rühmlichen proaktiven Orientierung und Investitionsbereitschaft in den Stand der Technik», laut Rickenbacher. Die Sensibilisierung und Notwendigkeiten rund um die Effizienzsteigerung mittels der Digitalisierung oder der Cybersicherheit würde wenigstens zunehmend erkannt und akzeptiert. Die Digitalisierung bzw. Transformation sei nicht aufzuhalten und damit auch die mit ihr verbundenen Risiken und Chancen. «Beten und Gottvertrauen rund um Cyber-Security reicht leider schon lange nicht mehr», mahnte Rickenbacher. Das sogenannte «Null-Vertrauen-Prinzip» (Zero Trust) in der digitalen Welt sei mitunter eine unumgängliche Grundregel geworden. Und hierzu gehöre auch das kritische Hinterfragen, Überprüfen oder Zurückfragen im Zweifelsfalle via bewusst einem anderen Kommunikations-Kanal wie z.B. dem guten alten Telefon!

«Wir dürfen nicht vergessen: die meisten sicherheitsrelevanten Probleme oder Ausgangspunkte für erfolgreiche Cyberangriffe entstehen nicht durch Technologie oder Maschinen, sondern die Schwachstelle ist oft der Mensch, meist aus Nachlässigkeit oder einer Art gefährlicher Systemgläubigkeit», erklärte Rickenbacher. Man müsse nur mal den Umgang mit Passwörtern oder Systemzugängen detaillierter studieren und man erkennt, dass Sicherheitslücken meist beim Menschen beginnen. «Bei leider immer noch unglaublichen rund 80 bis 90 Prozent aller Angriffe hilft der Anwender, sprich Mitarbeiter, aktiv unbewusst mit, den Angreifern ein mitunter fatales Erfolgserlebnis zu verschaffen.» Meist sei es ein zu schneller unbedachter, reflexartiger Klick auf einen Link, einen potenziell gefährlichen Anhang oder aber auch ein zu schwaches, nicht mit weiteren Faktoren geschütztes Passwort oder Systemzugang ohne weitergehende Schutzmassnahmen, was fatale Folgen habe auf die persönliche digitale Identität oder die gesamte Organisation / Firma.

> «Ein Idiot mit einem Plan schlägt ein Genie ohne Plan.»

«Cyber-Security und die entsprechende Mitarbeiter-Sensibilisierung ist nicht nur ein Status, sondern ein laufender, essentieller Prozess», betont Rickenbacher eingängig.

Aufruf an alle Akteure in der Firma: «Start thinking! Stop clicking!».

Der frühere, klassische Viren- und Firewall-Schutz habe längst ausgedient und sei nicht mehr auf dem «Stand der Technik». Die seit Jahren aktiven und leider unverändert erfolgreicher werdenden Angriffe wie Social Engineering, Phishing Mails oder vor allem auch sogenannte APT (Advanced Persistent Threat) bedürften einem Umdenken. Unternehmen müssten durch ihr Verhalten und laufenden Investitionen dafür sorgen, dass die Resilienz (Widerstandsfähigkeit) des Unternehmens gegenüber Systemausfällen oder Cyberangriffen erhöht werde. «Zuerst kritischer denken und erst danach ungestresst und korrekt handeln».

Im Weiteren empfiehlt und ermahnt Rickenbacher Folgendes: «Eine laufende, proaktive Orientierung zugunsten dem «Stand der Technik» mit z.B. Mitarbeiter-Cyber-Security-Re-Sensibilisierung, überwachter und automatisierter Endpunkt-Sicherheit (EDR / XDR), mehrstufiger Backup-Strategie, Identitäts-/Zugangs-Berechtigungs-Schutz bis hin zu gar «Security & Threat Intelligence» usw. sind mitunter auch Basis-Voraussetzungen für Compliance, Risk Management, Audits, Revisionen und Cyber-Security-Versicherungen.»

Kennwort- und Systemzugangs-Richtlinien und diese mit weiteren Faktoren besser schützen

Angriffe via gehacktes Passwort seien oft einfach, da Firmenanwender aus Bequemlichkeit im privaten und geschäftlichen Umfeld dieselben oder ähnliche, herleitbare Passwörter verwenden würden. «Solche Fehler wirken sich meist knallhart aus, bzw. werden schamlos ausgenutzt.» Sie liessen sich aber vermeiden: Etwa durch Systeme, die einen regelmässigen Wechsel bzw. überprüfen der Passwörter, Zugangsrechte und bei diesen eine vorgegebene Komplexität oder weiteren Prüf-Faktor (MFA, CA) erzwingen würden. Das Implementieren und auf dem «Stand der Technik» halten der nötigen Massnahmen und Tools in diesem Bereich und der sehr dynamischen Cyber-Security-Bedrohungslage sollte so selbstver-

Fridel Rickenbacher im Interview Marco Zörner (links).

ständlich sein wie der «Helm auf der ewigen Baustelle oder auf dem Velo».

Cyber-Security ist Chefsache und muss proaktiv geplant und verwaltet werden

Natürlich hätten die meisten Firmen inzwischen begriffen, wie anfällig die modernen Technologien und vor allem die Mitarbeiter auf Sicherheitsrisiken und Sicherheitslecks sind. Es gäbe aber leider auch immer noch viele Firmen, die glaubten, sie könnten sicherheitsrelevante Themen einfach und in «nur guter Hoffnung» an die Informatik-Abteilung delegieren. Dabei müsste sich das gesamte Management mit diesen Themen befassen – auch damit, wie man im Falle einer Cyberkrise reagiert mittels einer sogenannten Geschäfts-Kontinuitäts-Planung (BCP) bzw. Vorfall-Reaktionsplanung auf Sicherheitsvorfälle (IR).

«Unter der längst überfälligen Akzeptanz, dass Cyber-Security endlich zu den Top-Geschäfts-Risiken gehören sind entsprechende weitergehende Massnahmen unumgänglich. Ein fortwährend optimierter Schutz zugunsten der Angriffs- und Betriebssicherheit ist mittlerweilen eine interdisziplinäre Angelegenheit geworden unter Mithilfe und Involvierung von internen und externen Mitarbeitern und Partnern.» mahnt Rickenbacher. Aus einer IT-Planung über eine klassische IT-Strategie seien viele Organisationen übergegangen zu einer «eher agilen Strategie» aufgrund auch der hohen Dynamik in der Bedrohungslage, im Rahmen der Digital Transformation und den sprunghaften Technologie-Entwicklungen.

Typisch, die Informatik und vor allem die Cybersicherheit kommt meist erst am Schluss

Am Ende der langen GV konnte sich Rickenbacher folgende humorvoll betonte Aussage nicht verkneifen: «Ist wieder typisch, dass Cyber-Security erst am «Schluss» kommt und dann noch weniger Zeit als geplant erhält. Jetzt dürfen wir aber nur hoffen, dass wir aber halt in diesem verkürzten und gestressten «Schlussgang» nicht zu überrascht platt aufs Kreuz gelegt werden von Cybercrime bzw. unseren nicht gemachten, aber durchaus schon länger bekannten Hausaufgaben. Schon länger werden nicht nur die technischen IT-Diagramme, sondern viel mehr spezialisiert die Organigramme angegriffen mittels des Angriffsvektors «Social Engineering». Aus entsprechend nicht gemachten Hausaufgaben in der Informatik/Cyber-Security macht Cybercrime seit Jahren ein zunehmend lukratives Geschäftsmodell»