UNTERNEHMENSBEITRAG – INTERVIEW

«Ab jetzt müssen Hacker umdenken»

Ein effizienter Schutz vor Cyberangriffen und finanziellen Schäden ist für KMU unerlässlich. Wie das geht? Mit der Swiss Cyber Defence DNA. Thomas Liechti von MOUNT10 stellt diese Initiative vor.

IM INTERVIEW
Thomas Liechti
CEO, MOUNT10 AG
E: info@mount10.ch
www.mount10.ch

Herr Liechti, im ersten Halbjahr registrierte der Bund 85 Prozent mehr Cyberattacken. Worauf ist diese Explosion zurückzuführen?

Nicht die Firmen sind unsicherer geworden. Auch die Awareness ist in den vergangenen Jahren gestiegen. Man kann also nur mutmassen: Die einzige mir logisch erscheinende Erklärung ist, dass es anscheinend genügend Firmen gibt, die Lösegeld für ihre Daten bezahlen und damit den Hackern wieder mehr Mittel für neue Angriffe geben. Es muss also ein wirklich grosses Business rund um Schutzgeldzahlungen existieren, dass die Anzahl der Attacken so sehr nach oben schnellen.

Welche Auswirkungen hat dies für die betroffenen Unternehmen?

Gerade diejenigen Firmen, die vorher bereits in einer schwierigen Situation waren und dann durch einen Cyberangriff überrascht wurden, sind auf diese Weise in eine noch stärkere Schieflage geraten – mit der Folge, dass nun einige von ihnen nicht mehr am Markt vertreten sind. Das ist leider bereits mehrfach passiert. Besonders tragisch ist dies angesichts der hunderten Arbeitsplätze, welche davon betroffen sind.

Wo muss der Hebel zuerst angesetzt werden?

Wenn es etwas gibt, was essenziell und überlebenswichtig ist, dann ist dies ein robustes Backup. Es braucht ein Sicherheitsnetz, welches im Fall der Fälle tragen muss. Zwar gibt es keine 100-prozentige Sicherheit, jedoch müssen die Daten unveränderbar an irgendeinem sicheren Ort noch vorhanden sein.

Um diesen Angriffen vorzubeugen, haben Sie für KMU einen Best Practice Leitfaden zusammengestellt …

Ja richtig, grundsätzlich ist die Initiative von MOUNT10 ausgegangen. Letztlich erstellt haben wir die Swiss Cyber Defence DNA aber zusammen mit verschiedenen sehr gewichtigen Playern, wie Microsoft, Trend Micro, HPE, Cisco oder Swisscom. Als eine Non-Profit-Initiative haben wir einen Flyer gestaltet, welcher in guter, einfacher und verständlicher Sprache erklärt, wie man sich effizient gegen Gefahren der Cyber-Kriminalität schützen kann.

Welche Massnahmen sind das?

Diese reichen vom unveränderbaren Backup über den aktuellen Schutz vor Schadsoftware, wie Virenscanner und Firewall, bis hin zur Segmentierung und Absicherung von Netzwerken. Zudem geht es darum, Hard- und Software aktuell zu halten. Ziel ist es aber auch, mittels des Flyers einen Notfallplan im Unternehmen zu erstellen und Notfallprozesse zu definieren.

Oft rennen Unternehmen ihren Angreifern hinterher. Können sie mit diesen Massnahmen den Spiess umdrehen?

Wir sprechen hier von einem Wettrüsten. Unser Paket ist momentan in einem sehr guten Zustand. Wer sich an diesen Leitfaden hält, wird zumindest nicht tödlich getroffen. Aber es wird weitere Schritte brauchen, denn es gibt kein einziges Mittel, das immer vor einem Hacker schützt. Schlussendlich sind häufig die Mitarbeitenden die Schwachstellen. Auch sie machen Unternehmen verwundbar, etwa indem sie auf Links in E-Mails klicken, dem grössten Einfallstor von Cyberattacken. Dieses Verhalten kann man jedoch nicht komplett unterbinden – eine Schwachstelle, die es immer geben wird. Generell gilt: Im Zweifel nie!

«DIE MASSNAHMEN ZUM SCHUTZ VOR CYBERATTACKEN SIND VERSTÄNDLICH UND FASSBAR»

Wie können Unternehmen ihre Mitarbeitenden noch wachsamer machen?

Es ist eine Gratwanderung zwischen Sensibilisierung und Überdruss. Ein bis zweimal im Jahr sollten die Mitarbeitenden auf diese Gefahren angesprochen werden. Noch häufiger erachte ich als nicht sinnvoll, da dies das Gegenteil bewirken kann.

Was ist in der Cyberabwehr noch essentiell?

Wir, die Trägerschaft, unterstützen unsere Kunden beim Finden des geeigneten Umsetzungspartners. Letztendlich entscheidet aber der Kunde, mit wem er welche Massnahmen umsetzen möchte. Ziel unserer gemeinsamen Initiative ist es, den Nutzen für die KMU, den Schutz vor Erpressung, in den Vordergrund zu stellen.

Gibt es von Kundenseite bereits ein Feedback?

Immer mehr Kunden realisieren, agieren zu müssen. Und diejenigen, welche bereits die Massnahmen umgesetzt haben, nahmen diese weitaus weniger komplex wahr als gedacht. Im Gegenteil: Sie empfinden sie verständlich und fassbar. Ein Techniker eines grossen Umsetzungspartner half der Flyer sehr – auch weil er nun nicht mehr selbst den Kunden von der Notwendigkeit überzeugen muss, was zu tun ist. Nicht zuletzt betonte er, dass Reputationen der Trägerschaft dem Ganzen eine grosse Vertrauenswürdigkeit verleihen.

Weitere Informationen finden Sie auf kmuschutz.ch