UNTERNEHMENSBEITRAG – INTERVIEW

«So bleiben die Einfalltore für Hacker dicht»

Wie können sich KMU effizient gegen Cyber-Attacken und finanzielle Schäden schützen? Die Lösung: der neue Massnahmenkatalog, die Swiss Cyber Defence DNA. Thomas Liechti von MOUNT10 stellt ihn vor.

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

Herr Liechti, im vergangenen Halbjahr registrierte der Bund 85 Prozent mehr Cyberattacken. Worauf ist dieser extreme Anstieg 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? Was wird Ihnen berichtet?

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.

Damit es zu diesen Angriffen gar nicht erst kommt, 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.

«WER SICH AN DEN DNA-LEITFADEN HÄLT, WIRD ZUMINDEST NICHT TÖDLICH GETROFFEN»

Oft rennen Unternehmen ihren Angreifern hinterher. Ist es mit diesen Massnahmen möglich, einen Schritt voraus zu sein?

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 in Zukunft weitere Schritte brauchen. Nur so werden wir uns neuen Angriffsszenarien stellen können. Fakt ist: 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 nicht komplett unterbinden – eine Schwachstelle, die es immer geben wird.

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.

Raten Sie Unternehmen, Cyberattacken zu ver-sichern?

Es gibt mit Sicherheit Gründe, die für den Abschluss einer Versicherung sprechen. Jedoch kann es nur das Ziel sein, einen finanziellen Schaden abzusichern. Es gibt keine Versicherung die das Überleben oder die Daten schützt oder auch garantiert, diese wieder zurückzubekommen.

Inwieweit stehen Sie Ihren Kunden in der Cyber-abwehr noch zur Seite?

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.

WEITERE INFORMATIONEN UNTER:
www.kmuschutz.ch