So schützen sich KMU vor Cyber-Erpressung

Thomas Liechti
CEO Mount10 AG

Swiss Cyber Defence DNA (SCD-DNA) ist ein Leitfaden für KMU, mit dem sich Firmen einfach und effizient gegen Internet-Kriminalität absichern und grossen finanziellen Schaden abwenden können.

Als hätten KMU in der Coronapandemie nicht schon genug zu kämpfen, bleiben sie auch jetzt nicht von kriminellen Aktivitäten aus dem Netz verschont: Von einem Augenblick auf den anderen funktioniert das Emailsystem nicht mehr, Dateien lassen sich nicht mehr öffnen. Stattdessen fordert ein Totenkopf auf einem roten Bildschirm eine Bitcoin-Zahlung, während gleichzeitig ein Countdown startet. Ein Schreckensszenario für jedes KMU.

Diese Einführung mag etwas dramatisch klingen. Doch niemand, auch nicht KMU, ist vor den Gefahren von Cyberkriminellen geschützt. Und jede Firma, die auf die Erpressung eingeht, um die eigenen Daten wieder lesen zu können, finanziert damit die Machenschaften und die besseren Tools der Hacker. Lösegeld zu zahlen ist ähnlich sinnvoll, wie wenn man mit Benzin ein Feuer zu löschen versucht. Wer auf die Forderungen allerdings nicht eingeht, muss mit Datenverlusten rechnen.

Ansteckungsketten unterbrechen, was können KMU tun?
Da die Gefahren von Ransomware-Viren mit den richtigen, relativ einfachen Mitteln massiv eingedämmt werden können, wurde die «Swiss Cyber Defence – DNA»-Initiative ins Leben gerufen. Dabei handelt es sich um einen einfachen Leitfaden mit sechs Massnahmen (siehe Box), den KMU alleine oder mit Hilfe von Umsetzungspartnern abarbeiten können.

Was unterscheidet diesen Leitfaden von anderen online Checklisten?
Die Swiss Cyber Defence – DNA verzichtet darauf, dass KMU Daten eingeben müssen, um an die Informationen zu gelangen. Anhand der physischen Checkliste können KMUs die notwendigen Punkte abarbeiten, um auch die notwendige Übersicht zu behalten. Alle Informationen sind auch auf *www.kmu-schutz.ch* voll transparent einsehbar. Bei zusätzlichen Fragen stehen Umsetzungspartner in den Regionen zur Verfügung – auf dass die Hürden für Cyber-Kriminelle hoch und KMU weniger erpressbar werden.

www.mount10.ch

> **Niemand ist vor den Gefahren von Cyberkriminellen geschützt.**

Der folgende Massnahmenkatalog berücksichtigt die Verantwortungsbereiche Organisation und Technologie von Ihrem KMU gleichermassen.

Massnahme Nr. 1 - Aktuelle unveränderbare Datensicherung / schreibgeschütztes Backup
Ihre Überlebensfähigkeit als Firma sichern, ähnlich dem Airbag im Auto

- ☐ Eine Person für die Umsetzung und Überprüfung definieren
- ☐ Externe Speicherung des Backups sicherstellen
- ☐ Automatisierter, schreibgeschützter Backup-Prozess inkl. Verschlüsselung
- ☐ Wenn obiges nicht möglich: Backup-Medium vom Netzwerk trennen und offline lagern

Massnahme Nr. 2 - Umfassender und aktueller Schutz vor Schadsoftware
Dies ist Ihre erste Verteidigungslinie, wie eine sichere Haustüre

- ☐ Sensibilisierung und Schulung von Mitarbeitern im Umgang mit Emails, Webseiten, Passwörtern etc.
- ☐ Umfassender, flächendeckender Malwareschutz von Endgeräten, Servern, Cloud- und E-Mail Services
- ☐ Makroausführung einschränken; Internet- und Spamfilter installieren

Massnahme Nr. 3 - Netzwerke und Fernzugriffe absichern
Ihre Verteidigungsabschnitte für eine selektive Unterbindung nicht-autorisierter Zugriffe

- ☐ Schulung der Mitarbeiter und Lieferanten für Fernzugriff
- ☐ Netzwerke mittels Firewall in Zonen aufteilen, damit wichtige Geschäftsbereiche voneinander abgeschottet sind
- ☐ Fernzugriff mittels 2-Faktoren Authentifizierung zusätzlich absichern (z.B. SMS Code)

Massnahme Nr. 4 - Hardware und Software aktuell halten
Ihre Garantie für eine sichere, funktionierende IT

- ☐ Eine Person definieren, die für die Verwaltung und periodische Überprüfung der Lizenzen / Updates verantwortlich ist
- ☐ Gemäss Risikobeurteilung veraltete Systeme ablösen und bestehende physisch schützen (z.B. Zutritt zum Server)
- ☐ Nur aktuelle Betriebssysteme und Applikationen einsetzen
- ☐ Alte Systeme vom Netzwerk isolieren

Massnahme Nr. 5 - Mitarbeiter und deren Rollen
Ihr Selbstschutz mittels Einschränkung auf das Notwendige

- ☐ In einem Rollenkonzept definieren, welche Rechte pro Mitarbeiter notwendig sind
- ☐ Zugriffsrechte der Geschäftsleitung ebenfalls prüfen und einschränken
- ☐ Passwortregeln für Mitarbeitende erstellen
- ☐ Definierte Rollen mit den Zugriffsrechten koppeln und einschränken

Massnahme Nr. 6 - Notfallprozesse definieren
Ihre Absicherung in der Not mittels klar definiertem Plan anstelle von Improvisation

- ☐ Notfall-Organisation bestimmen, Prozesse definieren und alle Mitarbeiter informieren
- ☐ Rollen und Abläufe regelmässig überprüfen und Datenrückführung testen
- ☐ Unabhängige Technologie nutzen, um auch im Notfall auf die Dokumente zugreifen zu können (z.B. Notfall-Zettel, Ordner, Cloud oder Mobile Lösung)