Bild: Pete Linforth, pixabay.com

Mehr Cyber-Sicherheit durch starke Passwörter und 2FA

Der Diebstahl von Bitcoins im Wert von 1,5 Milliarden Dollar durch Nordkoreanische Hacker hat das Thema Cybersecurity im Februar 2025 schlagartig wieder ins Rampenlicht gerückt. Auch wenn bei Landtechnik-Unternehmen in der Regel keine riesigen Beträge zu holen sind, so sind auch sie konstant durch Cyberangriffe bedroht. Ransomware-Attacken, bei denen sämtliche Unternehmensdaten verschlüsselt werden, der Diebstahl vertraulicher Informationen oder betrügerisch ausgelöste Geldüberweisungen können auch im KMU verheerenden Schaden anrichten.

Keiner zu klein, um ein Hacking-Opfer zu sein

Bei KMU hält sich hartnäckig die Meinung, dass sie zu klein und damit kaum interessant für Hacker sind. Dabei macht sie genau dieser Umstand für Cyberkriminelle interessant. KMU nutzen oft ähnliche und nicht selten veraltete IT-Strukturen. Sie haben meist keine eigene IT-Abteilung, die sich regelmässig um Sicherheitsupdates, Antivirenprogramme und die Schulung der Anwenderinnen und Anwender kümmert. Hacker «justieren» ihre Lösegeldforderungen zudem und verlangen Summen, welche das angegriffene KMU gerade noch knapp verkraften kann.

IT in der Cloud heisst nicht automatisch sichere IT

Die Auslagerung des IT-Betriebes an einen externen Provider kann Vieles vereinfachen, vermittelt aber oft eine falsche Sicherheit. Wenn Hacker durch raffiniertes «Social Engineering» an das Zugangspasswort gelangen, können auch extern gespeicherte Daten und Backups verschlüsselt oder gestohlen werden.

Risiko Nummer 1: Sorgloser Umgang mit Passwörtern

Die beiden wichtigsten Einfallstore für Hacker sind schwache Passwörter und die Unaufmerksamkeit der Computer-Benutzerinnen und -Benutzer. Schwache Passwörter wie «Traktor777» oder der Name der Hauskatze werden von leistungsfähigen Rechnern innert Minuten geknackt. Besonders kritisch ist es, wenn dasselbe (schwache) Passwort für mehrere Accounts verwendet wird. Die wichtigsten Regeln für Passwörter lauten:

- Namen, Vornamen, Geburtsdaten, Telefonnummern oder Autokennzeichen sind tabu, weil diese Informationen öffentlich zugänglich sind.
- Keine real existierenden Wörter oder Begriffe verwenden.
- Das Passwort muss aus mindestens 12 Zeichen bestehen, Gross- und Kleinbuchstaben sowie Ziffern und Sonderzeichen (z. B. ç, &, *, /, $, ^) beinhalten. Ein Admin-Passwort

muss mindestens 16 Zeichen lang sein.
- Unterschiedliche Passwörter für unterschiedliche Konten verwenden. Zur Verwaltung mehrerer Passwörter kann ein Passwort-Manager wie z. B. «KeePass» verwendet werden. Aber Achtung: Wenn das Master-Passwort für den Passwort-Manager nicht konsequent geschützt wird, liegen auf einen Schlag sämtliche Passwörter des Unternehmens offen!
- Keine Passwörter in Excel-Listen oder Word-Dokumenten speichern. Diese sind für Hacker einfach auffindbar.
- Die besten Passwörter nützen nichts, wenn sie auf einem Post-it am Monitor kleben oder auf einem Zettel notiert sind, der von allen eingesehen werden kann.
- Passwörter müssen in regelmässigen Abständen geändert werden.

Zweifaktor-Authentifizierung aktivieren

IT-Provider, Bankdienstleister aber auch Webshops bieten meist die Möglichkeit, den Login durch eine Zweifaktor-Authentifizierung (2FA) zusätzlich abzusichern. 2FA kann mittels eines automatisch zugestellten SMS mit einem Zugangscode, spezielle Authentifizierungs-Apps wie z. B. den Google Authenticator oder auch mit Gesichts- oder Fingerabdruck-Erkennung erfolgen. Diese wirksame zusätzliche Schutzmassnahme kann beim Erstellen eines Kontos ausgewählt werden und lässt sich in der Regel auch im Nachhinein aktivieren.

Social Engineering zielt auf menschliche Schwächen

Eine verbreitete Methode von Cyberkriminellen ist das so genannte «Social Engineering», bei dem menschliche Eigenschaften und Schwächen gezielt ausgenutzt werden. Beispiel: Ein Buchhaltungsmitarbeiter erhält eine E-Mail eines Lieferanten. Der Absender teilt mit, dass eine Lieferung, welche der Chef dringend erwartet, erst versendet werden kann, wenn der offene Betrag in Höhe von CHF 22 500.– umgehend überwiesen wird. Eine Stunde nach Eingang der E-Mail drängt der «Lieferant» telefonisch erneut mit Nachdruck auf die Überweisung. Der Mitarbeitende will den Chef nicht verärgern und überweist den Betrag, der damit auf Nimmerwiedersehen verloren ist.

Wenn der Chef eine zackige E-Mail schickt

Eine weitere Spielart des Social Engineering ist der so genannte «CEO-Fraud» (Chef-Betrug), der auch als «Business E-Mail Compromise» (BEC) bekannt ist. In einem E-Mail, das vermeintlich vom Vorgesetzten stammt, wird der Empfänger aufgefordert, Geld zu überweisen oder Gutscheinkarten von Onlineshops zu kaufen und deren Codes per Mail zu senden. Gegen Angriffe mittels «Social Engineering» helfen vor allem Schulung und Sensibilisierung. Es kann auch sehr sinnvoll sein, festzulegen, bei welchen Geschäftsfällen zwingend eine Rückrufnummer vom Gesprächspartner angefordert werden muss. Auskünfte zu sensiblen Daten sollten generell nie telefonisch oder per E-Mail erteilt werden. Mitarbeitende müssen auch dafür sensibilisiert werden, dass sie sich durch die Preisgabe persönlicher Informationen auf Social Media zu Zielscheiben für «Social Engineering» machen können.

Weiter Tipps für mehr Datensicherheit im KMU

- **Ein Inventar der vorhandenen Hard- und Software erstellen**
  Nur so kann man beispielsweise herausfinden, ob das Unternehmen von einer neu bekannt gewordenen Sicherheitslücke betroffen ist.
- **Restriktive Zugriffsrechte**
  In der täglichen Arbeit sollten Mitarbeitenden nur über eingeschränkte Zugriffsrechten verfügen. Admin-Rechte müssen professionellen Systembetreuern vorbehalten sein.
- **Mitarbeitende für Phishing-Mails sensibilisieren**
  Mit Phishing wollen Cyberkriminelle an Zugangsinformationen gelangen oder Malware installieren. Typische Merkmale sind:
  - Versprechen von Gewinn oder Vorteilen beim Klick auf einen Link
  - Druck erzeugen, Angst machen (Androhung, dass z. B. die Kreditkarte gesperrt oder eine Sendung am Zoll blockiert wird)
  - Vorgaukeln einer amtlichen Stelle/Autorität (Polizei, Betreibungsamt o.ä.)
  - Fake URLs und E-Mail-Adressen. Diese sind oft schwer zu erkennen, da Kriminelle auch über gehackte Server seriöser Firmen operieren oder einen URL-Kürzungsdienst («https:/t.ly/xxxxxx») verwenden. Um das effektive Ziel eines Links anzeigen zu lassen, kann man mit dem Mauszeiger darüber fahren – nicht anklicken!
- **Software auf dem aktuellsten Stand halten**
  Veraltete Software ist eines der wichtigsten Einfallstore für Hacker.
- **Die Verwendung privater Geräte klar regeln**
  Wenn Mitarbeitende über private Mobilgeräte auf Unternehmensinformationen (Server oder Cloud) zugreifen, so braucht es klare Richtlinien. Das gleiche gilt für den Datenaustausch via USB-Sticks.

Eine Cyberrisk-Versicherung kann zusätzlichen Schutz bieten

Durch die Einhaltung der hier beschriebenen Regeln und insbesondere durch die Sensibilisierung des Teams kann Cyber-Gefahren im KMU besser begegnet werden. Einen absoluten Schutz gibt es angesichts der laufend weiterentwickelten Angriffsmethoden nicht. Ein zusätzliches Sicherheitsnetz kann eine spezielle Cyberrisk-Versicherung bieten, wie sie auch vom AM Suisse Versicherungspartner PROMRISK AG *(www.promrisk.ch)* angeboten wird. Die Betriebshaftpflichtversicherung deckt nämlich lediglich Personen- und Sachschäden, welche Dritten durch Verschulden des Versicherten entstehen. Vermögensschäden, die beim Kunden eines Landtechnikunternehmens entstehen, weil bei diesem Daten gestohlen wurden, sind nicht gedeckt. Die hohen Kosten, welche durch Betriebsunterbrüche, Ertragsausfälle, die Wiederherstellung der IT-Infrastruktur und allfällige juristische Auseinandersetzungen entstehen, sind in der Regel nur dann gedeckt, wenn eine spezielle Cyberrisk-Versicherung abgeschlossen wurde.

Emanuel Scheidegger