Schützen Sie Ihr Unternehmen vor Ransomware-Angriffen

Laut dem Official Annual Cybercrime Report 2019 wird alle 14 Sekunden ein Unternehmen Opfer von Ransomware. Wenn Mitarbeiter von zu Hause aus arbeiten und außerhalb der Firewall des Unternehmens tätig sind, steigt das Risiko.

Was ist Ransomware?

Bei Ransomware handelt es sich um bösartige Software, die den Benutzern den Zugang zu Computersystemen oder Geräten verwehrt, bis ein Lösegeld (Ransom) gezahlt wird. Diese Malware findet und verschlüsselt wertvolle Daten und sperrt Benutzer aus ihrem eigenen Betriebssystem aus. Dann wird im Gegenzug für den Entschlüsselungscode die Bezahlung von Lösegeld gefordert, üblicherweise in Form von Bitcoins oder anderen Kryptowährungen.

Darüber hinaus gibt es keine Garantie dafür, dass Betroffene nach der Zahlung des Lösegelds wieder Zugang zu ihren Geräte und Daten erhalten.

Sicherheitskopien und Aktualisierungen

Nutzen Sie mehrere Back-up-Lösungen und achten Sie darauf, dass zumindest eine davon immer offline ist. Hinweis: Cloud-Synchronisierungsdienste wie Dropbox oder Google Drive führen möglicherweise eine Synchronisierung durch, nachdem die Daten verschlüsselt wurden, was das entsprechende Back-up völlig nutzlos macht.

Aktualisieren Sie die Antivirensoftware des Unternehmens regelmäßig und wählen Sie einen Anbieter, der Add-ons anbietet, die Dateiverschlüsselung erkennen und automatisch Kopien der bedrohten Dateien erstellen.

Wählen Sie ein sicheres Passwort und ändern Sie es regelmäßig. Bedenken Sie, dass Brute-Force-Angriffe 31 Prozent aller Angriffe ausmachen.

Der Faktor Mensch

Schulen Sie Mitarbeiter darin, verdächtige E-Mails zu erkennen und zu melden – Ransomware kann sich leicht über Spam- und Fishing-E-Mails verbreiten.

Verwenden Sie Content-Scanning (Überprüfung von Inhalten) und E-Mail-Filter, um einen zusätzlichen Schutz zu gewährleisten. Diese Tools können bösartige Links erkennen und gefährliche E-Mails löschen, bevor sie die Mitarbeiter erreichen.

Sorgen Sie für ein standardisiertes Sicherheitsprotokoll im gesamten Unternehmen, von den Mitarbeitern bis zur Führungsebene.

Entwickeln Sie einen Notfallwiederherstellungsplan, der Reaktionen auf mögliche Angriffe beinhaltet. Berücksichtigen Sie technische Richtlinien, aber auch Strategien zur Abmilderung rechtlicher und rufschädigender Folgen.

Erkundigen Sie sich bei Ihrer Versicherung, ob Ihre Police die mit einem Ransomware-Angriff verbundenen Kosten abdeckt.

Erarbeiten Sie eine PR-Strategie, um Kunden, Investoren und der Presse die Situation im Falle eines Angriffs zu erklären.

Weitere Expertentipps zum Thema Cybersicherheit in Ihrer Smart Factory finden Sie im www.euautomation.com