Ransomware-Trojaner sind Schadprogramme die Ihre Daten verschlüsselt und damit den Zugriff auf die Dateien verwehren. Die Entwickler der Ransomeware fordern nach Platzierung der Trojaner Lösegeld, damit Ihre Daten wieder freigegeben werden. Das hört sich ein bisschen an, wie im wilden Westen und tatsächlich ist es auch der wilde Online-Westen. Häufig werden, aus Ermangelung anderer Alternativen, die Lösegeldforderungen bezahlt.
Gerade bei geschäftlichen Daten ist die Ransomeware ein Horrorszenario. Zudem wird es immer einfacher Ransomware zu erstellen. Durch Baukastensysteme haben selbst Personen ohne Programmierkenntnisse die Möglichkeit die Trojaner zu bauen und zu verteilen. Man kann also davon ausgehen, dass die Angriffe zukünftig noch gezielter und häufiger werden. Wir zeigen Ihnen wie Sie sich und Ihre Werkstatt bestmöglich schützen.

Wie kommt Ransomware auf meinen Computer?

Häufige Quelle sind Phishing Mails und Webseiten, also Fälschungen mit dem Ziel an Ihre Daten zu gelangen.

Wie können Sie Ihre Werkstatt vor Angriffen schützen?

Immer Updaten
„Oh nein, wieder ein Update…“ Ja, sie sind durchaus manchmal störend, lassen Sie dennoch keine Updates aus um Ihre Daten zu schützen. Veraltete Software durch fehlende Updates sind häufig Ursache von Schäden. Die Updates Ihrer Software schließen Sicherheitslücken nach bekanntwerden und können Sie so schützen.

Nur das Nötigste im Browser aktivieren
Großer Schwachpunkt der Sicherheit ist das Programm mit dem Sie häufig im Internet unterwegs sind, der Browser. Deaktivieren Sie unnötige Erweiterungen, Flash, Java etc.

Programminstallation
Viele Programme installieren Symbolleisten von Drittanbietern. Falls Ihnen Änderungen auffallen, sollten Sie das neuinstallierte Programm prüfen und ggf. löschen.

Aktuelle Virenschutzprogramme
Es gibt genügend kostenlose Virenscanner – Nutzen Sie sie und halten Sie diese immer aktuell um den Virenschutz aufrecht zu erhalten.

Regelmäßig Daten sichern
Vorsicht ist besser als Nachsicht: Führen Sie regelmäßig eine Datensicherung durch um im Ernstfall auf diese zurückgreifen zu können.
Es lohnt sich wirklich, denn so haben Sie im Notfall Zugriff auf halbwegs aktuelle Daten.

Nicht alles öffnen
Öffnen Sie nicht alles. Seien Sie besonders achtsam bei unbekannten Links und Dateien, überprüfen Sie die Anhänge von E-Mails vor dem Öffnen sorgfältig.
Vor allem, wenn Sie den Absender nicht kennen, sollten Sie keine offenen Dateiformate wie Word o.ä. öffnen.

Firewall
Erstellen Sie ein Firewall-Konzept für Ihr Netzwerk. Wenden Sie sich am besten dafür an Ihren IT-Fachmann des Vertrauens.

Auf dem Laufendem bleiben
Halten Sie steht’s Augen und Ohren offen. Was für Angriffe sind aktuell im Umlauf? Leiten Sie entsprechende Schutzmaßnahmen frühzeitig ein.

USB-Sticks achtsam nutzen
Auch über USB-Sticks kann Ransomeware auf Ihren Rechner gelangen. Seien Sie daher auch hier vorsichtig und nutzen Sie keine USB-Sticks deren Herkunft Ihnen unklar ist.

Ransomware auf dem Computer – Was tun?

Sind Sie Betroffener von Ransomware sollten Sie zunächst ein Foto von der Meldung machen und bei der Polizei Anzeige erstatten.

Danach können Sie auf verschiedener Weise handeln:
Sie können die letzte Datensicherung nutzen (wenn Sie diese regelmäßig durchgeführt haben) oder Sie befreien mit einem Entschlüsselungsprogramm das System bzw. suchen einen IT-Experten auf der Ihnen dabei helfen kann.

Nicht zu empfehlen ist die Zahlung für die Entsperrung.
Selbst wenn Sie zahlen gibt es keine Sicherheit, dass Sie im Anschluss tatsächlich wieder Zugang zu Ihren Daten erhalten. Im schlimmsten Fall, kann der Angreifer selbst die Daten nicht mehr entschlüsseln.

Also seien Sie achtsam und ergreifen Sie Schutzmaßnahmen um Ihre Werkstatt vor Angriffen zu bewahren. Frei nach dem Motto: Vorsicht ist besser als Nachsicht.