Trojaneralarm – lessons learned

Könnte sich das folgende Szenario auch in Ihrem Betrieb abspielen?

Dienstag 8:30 Uhr, der kaufmännische Angestellte bemerkt es als erster, mit seinem Computer stimmt etwas nicht. Nach dem Einschalten kann er seine Anwendung nicht starten, keine Serververbindung.

Dienstag 8:40 Uhr, sein Bildschirm wird blau und zeigt einen langen Text in großen weißen Buchstaben.

Dienstag 8:42 Uhr, der kaufmännische Angestellte ruft in der IT an. Das Telefon wird auf das Handy des IT-Leiters umgeleitet. Der sitzt im Auto und ist auf dem Weg.

Dienstag 10:45 Uhr, 2 Stunden später, in denen nichts ging, der IT-Leiter hat die Geschäftsleitung informiert und ruft nun bei seinem IT-Dienstleister an. Beide Server sind „blau“, wie er sich ausdrückt, ebenso ca. 80 Endsysteme. Nichts funktioniert, außer die Webseite. Die wird von einem externen Anbieter gehostet.

Das ist der GAU. Ein Verschlüsselungstrojaner hat die Systeme verschlüsselt. Der weiße Text bittet höflich um 100 Bitcoins (ca €99.000 stand Mai 2020) und verspricht nach Zahlung die Entschlüsselung der Systeme.

Dienstag 12:00 Uhr, ein Krisenstab wird gebildet. Experten arbeiten ab jetzt rund um die Uhr, um den Betrieb wieder her zu stellen. Der IT-Leiter hat unruhige Nächte.

Freitag 15:00 Uhr, die IT liegt nach 3 Tagen immer noch ab Boden. Die Geschäftsleitung entschließt sich, das geforderte Lösegeld zu bezahlen.
Der wirtschaftliche Schaden ist bereits enorm. Hinzu kommt der Verlust an Reputation bei Kunden und Partnern.
Ausgelöst wurde der Befall durch den Trojaner durch eine infizierte Webseite. Vermutlich hat ein Mitarbeiter nach dem Stichwort „Corona“ gesucht und ist unglücklicherweise auf diese Webseite gestoßen.

Lessons learned

Die Informationssicherheit in diesem Unternehmen hat offensichtlich Optimierungsbedarf, darum stelle ich 6 einfache Fragen.

1. Datensicherung: Für die beiden Server wird zwar eine tägliche inkrementelle Datensicherung durchgeführt. Beim Restore gab es aber ein Problem.Warum wurde der Restore nicht in regelmäßigen Abständen getestet?

2. Notfallkonzept: Warum dauert es 3 Arbeitstage, um dann festzustellen, dass man den Schaden nicht beheben kann und wohl oder übel doch das Lösegeld bezahlt?

(Im Übrigen rate ich von solchen Zahlungen ab. Die Realität zeigt, dass die Entschlüsselung in der Regel nicht oder nur sehr eingeschränkt funktioniert.)

3. Mitarbeitersensibilisierung: Sorgloses Surfen im Netz sollte für alle Mitarbeiter tabu sein. Wurden die Mitarbeiter nicht hinreichend geschult?

4. Virenschutz: Warum konnte die infizierte Webseite nicht vom Virenschutz auf dem Endsystem oder von einem Proxy blockiert werden?

5. Betriebssysteme und Anwendungen: Hat der Trojaner eine bereits bekannte Sicherheitslücke im Browser oder im System ausgenutzt? Hätte der Angriff durch ein regelmäßiges Update dieser Software verhindert werden können?

6. Sichere System- und Netzwerkkonfiguration: Warum konnte es dem Trojaner gelingen, sich vom Endsystem ausgehend auf beide Server und ca. 80 weitere Endsysteme auszubreiten? Konnte er vorhandene Sicherheitslücken in der Konfiguration der Systeme und des Netzwerks ausnutzen?

Jedes Unternehmen sollte ein Sicherheitskonzept etablieren und regelmäßig überprüfen. Diese 6 Fragen müssen darin umfassend behandelt werden.
Natürlich ist man im Nachhinein immer schlauer. Wichtig für die Informationssicherheit ist es, aus solchen Vorfällen zu lernen, Mängel im Sicherheitskonzept zu erkennen und diese zeitnah zu beheben. Wichtig ist hier das 4-Augenprinzip der Qualitätssicherung: das Sicherheitskonzept sollte von einem Experten betreut werden, der unabhängig von den internen und externen IT-Dienstleistern arbeitet und nur der Geschäftsleitung verantwortlich ist.

Wolf-IT-Architekt empfiehlt, ein Sicherheitskonzept nach dem Standard des BSI IT-Grundschutz zu etablieren. Das hat sich vielfach in der Industrie und in öffentlichen Institutionen bewährt. Als Teil des Systems sollten regelmäßige Informationssicherheits-Audits und Penetrationstests durchgeführt werden. Dadurch kann das einmal erreichte Niveau der Informationssicherheit auf Dauer gehalten werden.
Gerne übernimmt Wolf-IT-Architekt die Aufgabe eines IT-Sicherheitsbeauftragten, der das Sicherheitskonzept in Ihrem Unternehmen betreut und weiterentwickelt.