2024-07-21 Nur ein kleiner Fehler

Ein Weckruf für die Digitalisierung. Bisher war es ja noch immer gut gegangen, diesmal aber nicht. Es hätte jedoch auch noch viel schlimmer kommen können. Ein Umdenken und mehr Zeit und Geld für die Sicherheit wären jetzt wohl angebracht. (JDH)

Was ist passiert?

In einem automatischen Update einer Sicherheitssoftware von Crowdstrike war ein kleiner Fehler. Dieser Fehler führte beim Starten (Booten) des Rechners zu einem nicht ausführbaren Vorgang. Damit verabschiedet sich der Rechner von der weiteren Ausführung von Befehlen und führt nur noch ein Standard-Prozedere durch. Das bedeutet, es wird ein Fehlerprotokoll erstellt (Dump-File) und es wird der Blue Screen (Of Death) angezeigt und der Rechner „steht“.
Das neue Sicherheitsprogramm wurde bereits gestartet bevor das Hochfahren beendet war und man sich anmelden konnte. Somit wurde bei einem Neustart immer wieder das gleiche Ergebnis produziert und man kam nicht weiter.
Betroffen waren in der Regel nur größere Unternehmen. Jedoch gibt es auch Dienstleister, die für ihren kleineren Kunden ebenfalls diese Software eingesetzt haben. Privatpersonen waren in der Regel überhaupt nicht betroffen. Witzigerweise hatten ausgerechnet die Unternehmen Glück, die nicht die neuesten Windows-Versionen im Einsatz hatten, sondern mit alten, nicht mehr unterstützen Windows-Versionen arbeiten.
Insgesamt waren nur 1 % der Windows-Rechner betroffen, jedoch ein Großteil davon gehörten zur kritischen Infrastruktur, in Deutschland sogar zu KRITIS-Unternehmen, für die es besondere Sicherheitsanforderungen gibt.

Fehlerbeseitigung

Eigentlich ganz einfach. Jeder einzelne Rechner muss im abgesicherten Modus gestartet werden. Das bedeutet, das Betriebssystem startet nur sehr wenige Teile bzw. nur die unbedingt notwendigen Dienstprogramme. Somit wird auch der neue Fehler vermieden, da dieses Programm erst gar nicht gestartet wird. Trotz der eingeschränkten Möglichkeiten kann dann das fehlerhafte Programm entfernt bzw. durch eine fehlerfreie, neue Version ersetzt werden. Fertig.

Was ist nicht passiert?

So ziemlich alles, was an Bedrohungsszenarien möglich gewesen wäre, ist nicht eingetreten. Es wurden keine Rechner gekapert. Keine Daten wurden kopiert, verändert, gelöscht oder verschlüsselt. Kein Rechner konnte nicht wieder gestartet werden. Es wurden keine Passwörter abgeändert oder Zugänge verhindert.
Folgende aufwendige Tätigkeiten blieben aus:

- Neuinstallation von Rechnern
- Neuinstallation von Software
- Einrichten von Netzwerken
- Einrichten von Benutzern
- Neuvergabe von E-Mail (Konten und/oder Zugängen)
- Rückladen von Datensicherungen
- Nacharbeiten von Vorgängen bis zum Stand der Datensicherung
- Notbetrieb bis zur Wiederherstellung Normalbetrieb

Also unter dem Strich nur ein „kleiner“ Fehler mit großen Auswirkungen aber schneller Behebung.

Schuld und Sühne

Natürlich ist nicht Microsoft mit seinem Windows-Betriebssystem schuld, sondern der Softwarelieferant. Warum dieser Fehler vor der Auslieferung nicht entdeckt wurde, wird sich irgendwann zeigen. In der Regel sind die Softwareverträge so gestaltet, dass der Kunde die Software auf eigenes Risiko einsetzt und der Lieferant für nichts haftet. Jedoch sind natürlich Schäden eingetreten, die ersetzt werden sollten. Das wird natürlich die Anwälte und Gerichte beschäftigen. Auch die unterschiedlichen Versicherungen werden versuchen sich vor Zahlungen zu drücken.
Aber irgendwie sind wir alle ein wenig Schuld. Wir haben zugelassen, dass Microsoft 80% Marktanteil erreicht hat und somit ein Problem bei oder mit Microsoft immer große Auswirkungen nach sich zieht. Dazu wurde die IT-Sicherheit bei den Unternehmen vernachlässigt und teilweise auf Dienstleister übertragen. Generell wird bei der Digitalisierung immer Wert auf Preis, Funktionalität, und schnelle Einführung gelegt. Sicherheitsaspekte fallen da ganz schnell hinten runter, da diese nur Zeit und Geld kosten.

Fazit

Auf jegliche Fälle muss sich besser vorbereitet werden. Ein Notfallplan ist für jedes Unternehmen ein absoluter Standard, besser noch ein Geschäftsfortführungsplan mit entsprechenden Vorbereitungen und Vorbeugungsmaßnahmen um Schäden möglichst gering zu halten. Es fängt da schon mit einer vernünftigen Datensicherung an. Zudem sollte in jedem Unternehmen entsprechend Personal mit IT-Wissen vorhanden sein um einfache Probleme selber lösen zu können. Wenn ich als ein Kunde von mehreren tausenden Kunden eines Dienstleisten betroffen bin und alle Kunden das gleiche Problem haben, kann ich eine persönliche Unterstützung meines Dienstleisters vergessen.

Jochen D. Hohenwald