EMPFEHLUNG: IT IN DER PRODUKTION

Fallbeispiel Servicetechniker

Der Virus kommt zu Fuß!

Das BSI wurde von einem Betreiber einer verteilten Infrastruktur darüber informiert, dass es in mehreren Leitstellen vermutlich zu einem Virenbefall gekommen sei. Bei der weiterführenden Analyse und Behebung wurde daher um Unterstützung gebeten.

1 Was war geschehen?

Ein Servicetechniker hatte mehrere Leitstellen besucht und dort routinemäßige Arbeiten vorgenommen. Die arbeitsreiche Woche wollte er damit beenden, in der letzten zu besuchenden Leitstelle Anpassungen an der dort einzuspielenden Software vorzunehmen. Hierzu nutzte er den USB-Stick, mit dem er in den Tagen zuvor Aktualisierungen und Konfigurationsdaten in anderen Leitstellen aufgespielt hatte. Als er zur Vorbereitung den USB-Stick mit einem Entwicklungsrechner verband, löste die dort installierte Antiviren-Software einen Alarm aus: Auf dem USB-Stick war ein Schädling gefunden worden, der unterschiedliche Windows-Versionen zum Ziel hatte.

2 Wann geschah die Infektion?

Zur Eingrenzung der potenziell befallenen Leitstellen war es nun natürlich besonders wichtig herauszufinden, wann und wie die Infektion des USB-Sticks erfolgte. Der Virenschutz auf dem Entwicklungsrechner wurde täglich automatisch aktualisiert. Die zur Schadsoftware zugehörige Signatur war der Antiviren-Software bereits vor einigen Wochen bekannt gewesen. Das letzte Mal hatte der Servicetechniker den USB-Stick vor einigen Tagen mit diesem Entwicklungsrechner verbunden. Dabei war keine Warnung ausgelöst worden.

Nach einem ersten Gespräch des Servicetechnikers mit Kollegen machte dieser am Abend eine unangenehme Entdeckung. An seinem privaten PC wurde nach einer Aktualisierung der Antiviren-Software die gleiche Malware gefunden. Dies führte dazu, dass er am folgenden Tag ein folgenschweres Versäumnis einräumen musste: 24 Stunden vor der Abreise zu den verschiedenen Leitstellen hatte er den USB-Stick noch einmal kurzerhand mit dem privaten PC verbunden, um eine Auswahl seiner mp3-Sammlung während der Reise im PKW hören zu können. Es erhärtete sich der Verdacht, dass hierbei die Infektion erfolgt war. Zunächst war es nun erforderlich, die potenziell betroffenen Leitstellen einzugrenzen. Diese hatten allesamt Windows-Versionen im Einsatz, die von der Schadsoftware hätten infiziert werden können.

3 Also, was tun?

Eine einfache Beseitigung der Schadsoftware mit der durch das Antiviren-Programm angebotenen Option – wie auf einem privaten PC oder dem Entwicklungsrechner – war nicht möglich: Aufgrund von Echtzeitanforderungen und regulatorischen Vorgaben konnte Antiviren-Software nicht auf den Systemen in der Leitstelle betrieben werden. Daher war zunächst nicht einmal sicher, ob die Systeme überhaupt mit der Schadsoftware infiziert waren oder nicht. Es blieben die folgenden Optionen für das weitere Vorgehen:

Einer der Mitarbeiter des Betreibers schlug vor, eine Analyse der Schadsoftware vornehmen zu lassen, um deren potenzielle Auswirkungen beurteilen zu können. Falls eine Auswirkung auf die Funktionsfähigkeit der Leitstelle ausgeschlossen werden könne, so müsse man die Schadsoftware nicht entfernen. Diese Option wurde verworfen, da hierzu die Zeit nicht ausreichte und auch keine qualifizierten und vertrauenswürdigen Firmen bekannt waren, die eine solche Analyse hätten durchführen können.

Alternativ kam eine Neuinstallation der (potenziell) betroffenen Systeme infrage. Nach einer Schätzung der resultierenden Aufwände und der vermutlichen Dauer des Ausfalls der Leitstelle wurde diese Option auch verworfen, zumal kein hinreichendes Notfallmanagement etabliert war und nicht einmal sämtliche Softwarekomponenten, Konfigurationsdaten und Anlagendokumentation zeitnah zur Verfügung standen. Auch war ja noch immer nicht verifiziert, dass die Systeme der Leitstelle überhaupt infiziert waren.

Schließlich schlug der Servicetechniker vor, entgegen den geltenden Regelungen und Vorgaben kurzzeitig eine Antiviren-Software in der Leitstelle zu installieren und diese nach erfolgreicher Prüfung und ggf. Entfernung der Software wieder zu deinstallieren. Die Verantwortlichen waren sich schnell einig darüber, dass dies evtl. funktionieren könnte. Nach einer langwierigen Diskussion über die unkalkulierbaren Risiken bzgl. der Verfügbarkeit und Stabilität der Leitstelle sowie die Frage, ob die Leitstelle nach einem Neustart im Anschluss an die Installation bzw. Deinstallation noch funktionieren würde, wurde die Lösung dann aber auch verworfen.

Schließlich wurde nach Abstimmung mit dem Integrator der Anlage entschieden, eine Virenschutz-Lösung zu verwenden, die keine Installation auf dem betroffenen System erfordert und – abgesehen von einer eventuellen Bereinigung – keine Veränderungen vornimmt. Auch bestanden Restrisiken, die von den Verantwortlichen aber notgedrungen übernommen wurden. Die Suche ergab, dass einige der Systeme von der Schadsoftware infiziert worden waren.

Bei der weitergehenden Analyse ergab sich aber, dass der Betreiber eine wichtige Sicherheitsmaßnahme bereits umgesetzt hatte: Aus der Leitstelle war keine Kommunikation mit dem Internet möglich. Dies führte vermutlich dazu, dass die Schadsoftware keinen Kontakt zu einem sogenannten Command & Control Server aufnehmen konnte, um an diesen Daten abfließen zu lassen oder weitere Anweisungen entgegenzunehmen.

4 Lessons learned

4.1 Was hätte in diesem Fall anders laufen müssen?

- Die Sensibilisierung nicht nur der Mitarbeiter, sondern speziell auch von externen „Experten“, muss darauf hinwirken, dass diese mit der gebotenen Vorsicht mit den IT-Systemen umgehen.
- Es müssen verbindliche Policies, auch für externe Experten, zur Nutzung von IT festgelegt werden, die u. a. eine berufliche und gleichzeitig private Nutzung von IT-Komponenten verbieten.
- Es muss ein Notfallmanagement etabliert werden – insbesondere mit Blick auf die Wiederherstellung von Systemen.

- Es sollten PCs mit aktuellem Virenschutz zur Prüfung von Wechseldatenträgern genutzt werden, bevor diese mit Steuerungskomponenten verbunden werden ("Wechseldatenträgerschleuse"). Ein solcher Virenschutz am Perimeter hat den Vorteil, dass hieraus keine möglichen Beeinträchtigungen für die Steuerungskomponenten selbst resultieren. Die Nutzung sollte auch für externe Experten vorgeschrieben werden.
- Eine Beschränkung der verwendbaren Wechseldatenträger mittels Bordmitteln des Betriebssystems oder durch sogenannte Device Control Produkte kann die Wahrscheinlichkeit eines solchen Vorfalls verringern.

4.2 Was war gut?

Es sollte keine direkte Kommunikation zwischen IT-Systemen in der Leitstelle und dem Internet möglich sein.

5 Resümee

Bei Wartungstätigkeiten kommt es immer wieder zu Infektionen mit nicht-zielgerichteter Malware. Dies betrifft sowohl Wartungstätigkeiten vor Ort mit USB-Stick oder Wartungsnotebook als auch die Fernwartung über das Internet. Eine solche Infektion kann jedoch die Funktionalität und Verfügbarkeit einer Anlage massiv beeinträchtigen. Eine Behebung ist – je nach bestehenden Rahmenbedingungen – mitunter sehr schwierig. Daher sollten Anlagenbetreiber dringend die zuvor genannten Empfehlungen berücksichtigen.

6 Weitere Informationen

Als weiterführende Literatur zu den Cyber-Sicherheitsbedrohungen industrieller Anlagen bietet sich u. a. das Dokument "Top 10 ICS Bedrohungen und Gegenmaßnahmen" an. Als Grundlage für die Absicherung von Steuerungen und Industrieanlagen eignet sich das ICS Security Kompendium des BSI. Diese und weitere Dokumente sind verfügbar unter:

https://www.bsi.bund.de/ICS-Security-Kompendium

Mit den BSI-Veröffentlichungen publiziert das Bundesamt für Sicherheit in der Informationstechnik (BSI) Dokumente zu aktuellen Themen der Cyber-Sicherheit. Kommentare und Hinweise können von Lesern an **info@cyber-allianz.de** gesendet werden.