Patchmanagement

Problembeschreibung und Ursache

Es werden fast täglich für die verschiedensten IT-Komponenten neue Schwachstellen bekannt, die geschlossen werden müssen. Auch die OT ist von Schwachstellen auf sowohl der Software- als auch der Hardware-Ebene nicht unversehrt. Um diese Schwachstellen schließen zu können, müssen auf der jeweiligen Soft- bzw. Hardware Sicherheitspatches eingespielt werden.

Bedrohungsszenarien

Im Gegensatz zu den Zero-Days, die bereits in Level Schadsoftware thematisiert wurden, werden für Schwachstellen, die öffentlich bekannt sind, oft Sicherheitspatches von den Herstellern angeboten. Dies muss aber nicht immer der Fall sein, wobei man hierbei auf andere Ausgleichsmaßnahmen zurückgreifen muss. Sind jedoch Sicherheitspatches für Schwachstellen vorhanden, ist es entscheidend, von diesen Sicherheitspatches Bescheid zu wissen und diese schnellstmöglich zu installieren. Daher ist es von großer Bedeutung, dass man sich regelmäßig über neue Patches für das ICS-System informiert. Vernachlässigt man dies, können Hacker das ICS-System auf ihre Versionsnummer überprüfen und damit nach öffentlichen Schwachstellen und Exploits suchen. Je nach Schweregrad der Schwachstelle kann dies einen großen Schaden anrichten.

Gegenmaßnahmen und Sicherheitsvorkehrungen

Authentizität und Integrität

Es ist wichtig, Sicherheitspatches auf ihre Authentizität und Integrität zu prüfen. Es gibt unterschiedliche Liefermechanismen für Patches, wie z.B. über Netzwerkübertragung, CD/DVD oder USB-Sticks. Der Patch kann jedoch während der Übertragung abgefangen werden und mit Schadsoftware infiziert werden. Daher ist es wichtig, der Verteilungsweg zu schützen und eine Integritätsprüfung mithilfe von digitalen Signaturen durchzuführen.

Validierung und Installation

Es muss ebenfalls geprüft werden, dass der Sicherheitspatch mit dem ICS kompatibel ist. Da Sicherheitspatches oft unabhängig vom ICS entwickelt werden, kann es sein, dass der Patch nicht mit dem ICS kompatibel ist. Wird der Patch dennoch installiert, kann dies massive Auswirkungen auf die Funktionalität des ICS haben. Um dies zu vermeiden, sollte der Patch, meist vom Hersteller, vor der Verwendung in einem Gerät geprüft werden. Da das ICS aber in der Zeit angreifbar ist, ist eine rechtzeitige Installation von großer Bedeutung. Vor der Installation sollten ebenfalls Tests durchgeführt werden und die Updates sollten am Besten sequenziell installiert werden. Hierbei sollten redundante Systeme zuerst bespielt werden. Vor dem Einspielen von Patches sollten optimalerweise Datensicherungen für jedes ICS durchgeführt werden.

Statuserfassung

Der Status der Sicherheitspatches aller Geräte sollte dokumentiert und aktuell gehalten werden. Dies ist bei der Fehlersuche oder Diagnose von großem Vorteil. Zudem ist es bei der Berurteilung von Schwachstellen eines Geräts wichtig zu wissen, welche Sicherheitspatches angewendet wurden. Der Status soll mindestens beinhalten:

- Patchkennung
- Anwendbare Software
- Datum der Patchfreigabe und Installation

Beibehaltung der Sicherheit

Es kann passieren, dass durch die Installation von Patches die Sicherheit der Geräte verringert wird. Zum Beispiel können Sicherheitspatches bekannte Schwachstellen einführen, bestimmte Konfigurationseinstellungen entfernen oder die Funktion der Software ändern. Daher muss überprüft werden, ob der Zustand des Inhalts und der Konfiguration eines Geräts durch den Patch nicht beeinträchtigt wurde.

Fehlende Sicherheitspatches

Wird eine Schwachstelle bekannt, doch es gibt (noch) keinen Sicherheitspatch, so muss in einer Risikoanalyse alternative Maßnahmen betrachtet und ergriffen werden, um die Ausnutzung der Schwachstelle zu verhindern. Als alternative Maßnahme ist es z.B. möglich, die betroffenen ICS in ein separates Netzsegment zu setzen und den Datenverkehr zu diesem Netzsegment mit einer Firewall zu filtern.

Dieses Dokument orientiert sich an der IEC-62443-2-1 Norm, insbesondere die Komponente SPE4 - Komponentensicherheit: COMP3 - Patchmanagement