Netzwerksegmentierung

Problembeschreibung

Die Struktur und der Aufbau des OT-Netzwerkes ist der wohl wichtigste Bestandteil der OT-Security. Ohne eine gut durchdachte Netzwerksegmentierung kann es für Hacker ein Kinderspiel sein, in das OT-Netz einzudringen. Bei vielen Industrieanlagen sind IT- und OT-Netz voneinander getrennt, doch diese zwei Netzwerke wachsen immer mehr zusammen, da dies viele Vorteile bringt. Die einfachste Vorgehensweise hierbei wäre es, das IT- und OT-Netz direkt miteinander zu verbinden, ohne jegliche Sicherheitsvorkehrungen. Zudem wurden die meisten OT-Netzwerke flach gebaut, das heißt dass alle Geräte uneingeschränkt miteinander kommunizieren können.

Bedrohungen

Die direkte Verbindung von OT und IT sowie die flache Netzwerkstruktur im OT-Netz birgt natürlich gewisse Gefahren. So gab es z.B. schon Fälle, in denen Unternehmen bestimmte Geräte in ihrem ICS so konfiguriert haben, dass diese aus dem Internet erreichbar sind. Dies sollte man aber um jeden Preis vermeiden, da solche ICS-Geräte und ihre IP-Adressen online auf Suchmaschinen wie z.B. Shodan zu finden sind. Sind diese Geräte dann mit z.B. Standard-Passwörtern unsicher konfiguriert, ist es für einen Hacker schon zu einfach, in das OT-Netz einzudringen. Ist das OT-Netz zudem mit einer flachen Netzwerkhierarchie konstruiert, hat der Hacker uneingeschränkten Zugriff auf das gesamte OT-Netzwerk.

Netzwerkstrukturen

Im Folgenden werden einige Netzwerkstrukturen und ihr Sicherheitsniveau behandelt.

Flache Netzwerkhierarchie:

In einer flachen Netzwerkhierarchie existiert keine Form von Segmentierung. Wie oben schon erwähnt, können in diesem Fall alle Geräte uneingeschränkt miteinander kommunizieren. Dadurch haben Hacker, die in das OT-Netz eingedrungen sind, vollen Zugriff auf alle Systeme. Sind IT- und OT-Netz zudem noch miteinander verbunden, was heutzutage immer populärer wird, kann ein Hacker durch das Infizieren des IT-Netzes auch Zugriff auf das OT-Netz erhalten. Ein einfaches Trennen der Netzwerke mit einer Firewall reicht hierbei nicht aus, da eine Workstation, für die die Kommunikation mit dem OT-Netz erlaubt ist, von einem Hacker infiziert und ausgenutzt werden kann.

VLANs:

Das OT-Netz kann mit der Implementierung von VLANs sicherer gemacht werden. Durch die Segmentierung mit VLANs werden Netzwerkelemente logisch gruppiert, sodass die Kommunikation zwischen den VLANs abgesichert werden kann, was einer Malware-Verbreitung im Netzwerk entgegen wirkt.

Mikro-Segmentierung:

Die Mikro-Segmentierung sorgt für den höchsten Schutz des OT-Netzes. Es erweitert die VLAN-Segmentierung um ein weiteres Sicherheitsfeature. Die einfache VLAN-Segmentierung birgt noch ein Risiko innerhalb eines VLANs. Innerhalb eines VLANs wird die Kommunikation zwischen den Geräten nicht überwacht oder überprüft, was eine Angriffsfläche für die Verbreitung von Malware bietet. Mithilfe der Mikro-Segmentierung jedoch wird diese Schwachstelle behoben. Durch die Verwendung einer Next-Generation-Firewall (NGFW), wie z.B. die von Fortinet, lässt sich eine Zero-Trust-Security implementieren, bei der der gesamte VLAN-Datenverkehr überprüfen lässt. Somit lassen sich Sicherheitsregeln für die interne Kommunikation innerhalb eines VLANs umsetzen.

Gegenmaßnahmen und Sicherheitsvorkehrungen

Netzwerkautonomie

Das ICS muss autonom sein, d.h. es sollte bei der Trennung von externen Netzwerken wie vorgesehen funktionieren können. Dadurch verhindert man, dass durch einen Ausfall in einem externen Netzwerk ebenfalls ein Ausfall im ICS entsteht. Um diese Netzwerkautonomie zu erreichen, sollte man potenziell in Kauf nehmen müssen, dass das ICS dadurch in einem verschlechterten oder weniger optimierten Modus betrieben werden muss.

Nachrichtenaustausch

Nachrichten, die im ICS-Netz übertragen werden, sollten keine Nutzlasten wie z.B. Anhänge enthalten, da diese Schadsoftware einschleusen können. Zudem könnten diese Nachrichten Links zu nicht vertrauenswürdigen Seiten beinhalten. Daher sollten E-Mail, Instant Messaging usw. von der Verwendung im ICS ausgeschlossen werden.

Zeitverteilung

Die Zeitquellen, die für die sichere Verteilung und Synchronisierung der Zeit innerhalb des ICS verwendet werden, sollten vor Manipulationen geschützt werden. Die genaue und systemweite Zeit wird zur Zeitstempelung von Ereignissen verwendet und ist wichtig für die Nachvollziehbarkeit bei Fehlern oder Angriffen. Daher sollte ein Zeitverteilungsprotokoll verwendet werden, das für industrielle Anwendungen allgemein akzeptiert wird.

Dieses Dokument orientiert sich an der IEC-62443-2-1 Norm, insbesondere die Komponente SPE3 - Netzwerk- und Kommunikationssicherheit: NET1 - Systemsegmentierung sowie einem Dokument von Fortinet zur “Security für OT-Netzwerke mit Mikro-Segmentierung (https://www.fortinet.com/content/dam/fortinet/assets/solution-guides/de_de/sb-securing-ot-networks-with-microsegmentation.pdf)