Netzwerksegmentierung

Netzwerkstrukturen

Flache Netzwerkhierarchie:

In einer flachen Netzwerkhierarchie sind IT- und OT-Netz miteinander verbunden und es existiert keine Netzwerksegmentierung. Dadurch können Hacker bei einer Infizierung des IT-Netzes direkt in das OT-Netzwerk vordringen. 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.

Segmentierung von nicht-ICS-Netzwerken

Da externe Netzwerke den Zugang zum ICS aus potenziell unbekannten Quellen ermöglicht, sollte darauf geachtet werden, dass Segmentierungs- und Kommunikationsrichtlinien durchgesetzt werden. Durch diese Netzwerksegmentierung ist es möglich, den Verkehr und die Sichtbarkeit zwischen ICS und externen Systemen einzuschränken. Dieser Verkehr sollte zudem identifiziert, verwaltet, autorisiert und dokumentiert werden. Um die Datenflüsse zu autorisieren, sollten Netzwerksicherheitsgeräte zwischen ICS- und Nicht-ICS-Segmenten verwendet werden.

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.

Benutzer-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.

Netzwerkzeitverteilung

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)