Vulnerability Management in hochkritischen Umgebungen

ausführlichere Beschreibung des Vortrags:

Sowohl Hardware- als auch Softwarekomponenten eines industriellen Netzwerks unterscheiden sich wesentlich von klassischen Office- und Serverumgebungen. Das Ziel der Verfügbarkeit ist in diesen Umgebungen in der Regel deutlich höher priorisiert als die Sicherheitsziele Vertraulichkeit und Integrität. Obwohl die Auswirkungen eines Ausfalls dieser Komponenten meist einen immensen Schaden inklusive höherem Reparaturaufwand bedeutet sind diese Systeme nahezu immer mit sehr alten Softwareständen ausgestattet. Da jegliche Veränderung dieser fragilen Systeme ein potentielles Risiko für Produktionsumgebungen darstellt müssen andere Techniken zur Angriffserkennung und Schwachstellenanalyse angewendet werden. Hierbei stellen passive Vulnerability Scanner den aktuellen Stand der Technik dar. Die von den Tools verwendete technische Komponente nennt sich Deep Packet Inspection, welche qualitativ hochwertiges, passives Netzwerkmonitoring ermöglicht und über die Grenzen von industriellen Netzwerken hinaus einsetzbar ist. Besucher des Vortrags sollen einen Einblick in die Technik von passiven Scannern bekommen, welche zu einer sehr hohen Transparenz in Netzwerken führen kann. Die vom vortragenden Analysten gesammelten Erfahrungen während eines innerbetrieblich durchgeführten Proof of Concepts werden erläutert und die den kommerziellen Produkten zugrunde liegenden Open Source Komponenten vorgestellt.

erforderliches Vorwissen:

Grundwissen über Netzwerke und Betriebssysteme. Grundwissen über Schwachstellenscanner sind von Vorteil werden aber nicht vorausgesetzt.

Webseiten von Herstellern passiver Vulnerability Scanner:

https://cyberx-labs.com/de/
https://www.darktrace.com/en/
https://www.nozominetworks.com/
https://www.indegy.com/
https://de.tenable.com/indegy?tns_redirect=true
https://www.forescout.com/platform/operational-technology/

Literatur zum Thema:

Hacking Exposed Industrial Control Systems: ICS and SCADA Security Secrets & Solutions
https://www.amazon.de/Hacking-Exposed-Industrial-Control-Systems/dp/1259589714

Network Forensics
https://www.amazon.de/Network-Forensics-Ric-Messier/dp/1119328284/ref=sr_1_6?__mk_de_DE=%C3%85M%C3%85%C5%BD%C3%95%C3%91&keywords=network+forensics&qid=1578512272&sr=8-6

Network Forensics: Tracking Hackers Through Cyberspace
https://www.amazon.de/Network-Forensics-Tracking-Hackers-Cyberspace/dp/0132564718/ref=sr_1_9?__mk_de_DE=%C3%85M%C3%85%C5%BD%C3%95%C3%91&keywords=network+forensic&qid=1578512349&sr=8-9

Abstract in Programmheft:

Sowohl Hardware als auch Software Komponenten eines industriellen Netzwerks unterscheiden sich wesentlich von klassischen Office- und Serverumgebungen. Das Ziel der Verfügbarkeit ist in diesen Umgebungen in der Regel deutlich höher priorisiert als die Sicherheitsziele Vertraulichkeit und Integrität. Obwohl die Auswirkungen eines Ausfalls dieser Komponenten meist
einen immensen Schaden inklusive höherem Reparaturaufwand bedeutet sind diese Systeme nahezu immer mit sehr alten Softwareständen ausgestattet. Da jegliche Veränderung dieser fragilen Systeme
ein potentielles Risiko für Produktionsumgebungen darstellt müssen andere Techniken zur Angriffserkennung und Schwachstellenanalyse angewendet werden. Hierbei stellen passive Vulnerability Scanner den aktuellen Stand der Technik dar. Die Funktionsweise, die Einsatzmöglichkeiten und die Grenzen dieser Technik soll anhand der Resultate eines im Betrieb durchgeführten Proof of Concepts aufgezeigt werden.