Security-Richtlinie

SIMA² Master Station

Erste Veröffentlichung: 2022-05-23

Letztes Update: 2022-05-23

Zweck dieser Security-Richtlinie

Steuerungssysteme und Steuerungsnetzwerke wie die SIMA² sind Cyberbedrohungen ausgesetzt. Um diese Risiken zu minimieren, stehen die unten genannten Schutzmaßnahmen zusätzlich zu weiteren Maßnahmen zur Verfügung. AUMA ruft Systemintegratoren und Anlagenbesitzer dazu auf, geeignete Schutzmaßnahmen für ihre Steuerungssystemumgebung zu realisieren.

Empfehlungen für die SIMA² Master Station

- Binden Sie die SIMA² Master Station in dedizierte Netzwerke ein, welche nur Steuerungssysteme beinhalten.
- Schützen Sie Steuerungsnetzwerke und -systeme durch Firewalls und separieren Sie diese von allen anderen Netzwerken wie Unternehmensnetzwerken und dem Internet.
- Blockieren Sie jeglichen eingehenden Internetverkehr, der versucht, auf die Steuerungsnetzwerke/Steuerungssysteme zuzugreifen. Stellen Sie Fernzugriffssysteme, die für den Fernzugriff auf Steuerungssysteme verwendet werden, außerhalb des Steuerungsnetzwerks auf.
- Beschränken Sie den von den Steuerungssystemen/Steuerungsnetzwerken ausgehenden Internetverkehr auf das Nötigste. Wenn Steuerungssysteme mit dem Internet verbunden werden müssen, passen Sie die Firewall-Regeln an die erforderlichen Ressourcen an. Lassen Sie nur Quell-IPs, Ziel-IPs und Dienste/Ziel-Ports zu, welche die Steuerungssysteme für den normalen Steuerungsbetrieb unbedingt verwenden müssen.
- Sollte ein Internetzugriff nur gelegentlich notwendig sein, so können Sie die entsprechenden Firewall-Regeln deaktivieren und nur während der Zeitspanne aktivieren, in welcher der Internetzugang benötigt wird. Sofern Ihre Firewall dies unterstützt, definieren Sie ein Ablaufdatum und Ablaufzeit für derartige Regeln. Nach dem Ablaufdatum und der Ablaufzeit wird die Firewall diese Regel automatisch deaktivieren.
- Setzen Sie die Steuerungsnetzwerke/die Steuerungssysteme nur begrenzt dem Zugriff interner Systeme aus. Passen Sie die Firewall-Regeln, die Datenverkehr von internen Systemen zu Steuerungsnetzwerken/Steuerungssystemen zulassen, so an, dass nur Quell-IPs, Ziel-IPs und Dienste/Ziel-Ports zugelassen werden, die für den normalen Steuerungsbetrieb unbedingt erforderlich sind.
- Erstellen Sie strenge Firewall-Regeln, um bösartigen Netzwerkverkehr zu filtern, der auf Schwachstellen im Steuerungssystem abzielt („Exploit Traffic“). Der Exploit Traffic kann Netzwerkkommunikationsfunktionen wie Source-Routing, IP-Fragmentierung und/oder IP-Tunneling nutzen. Sollten solche Funktionen für den normalen Steuerungsbetrieb nicht notwendig sein, so blockieren Sie diese auf Ihrer Firewall.
- Setzen Sie Intrusion Detection Systems (IDS) oder Intrusion Prevention Systems (IPS) zur Erkennung/Blockierung von steuerungssystem-spezifischem Exploit Traffic ein. Erwägen Sie die Verwendung von IPS Regeln, die zum Schutz gegen Exploits von Steuerungssystemen dienen.
- Sollte ein Fernzugriff notwendig sein, nutzen Sie sichere Verbindungen wie beispielsweise VPN-Verbindungen (Virtual Private Networks). Stellen Sie sicher, dass die VPN-Lösungen immer auf dem neuesten Stand sind.
- Wenn Sie den internen Steuerungsnetzwerkverkehr filtern möchten, erwägen Sie bitte die Verwendung von Lösungen, die Intra-LAN-Verkehrssteuerung wie VLAN -Zugriffskontrolllisten unterstützen.
- Sichern Sie Ihr Steuerungssystem durch exklusive Freigabe nur der Ports, Dienstleistungen und Software ab, die für den normalem Steuerungsbetrieb benötigt werden.
- Beschränken Sie die Berechtigungen von Benutzerkonten, Softwareprozessen und Geräten nach Möglichkeit auf die im normalen Steuerungsbetrieb erforderlichen Berechtigungen.
- Verwenden Sie vertrauenswürdige, gepatchte Software und Lösungen zum Schutz vor Malware. Interagieren Sie nur mit vertrauenswürdigen Websites und vertrauenswürdigen E-Mail-Anhängen.
- Schützen Sie die Steuerungssysteme vor dem physischen Zugriff durch Unbefugte, z. B. durch Unterbringung der Systeme in verschlossenen Schaltschränken.