EDGE Device
Security Paper

ENGEL
be the first

Technische Sicherheit

TPM

Das EDGE Device hat einen TPM 2.0 Chip verbaut. Dieser wird für kryptografische Operationen wie z.B. das Ablegen von Schlüsseln verwendet. Unter anderem wird dieser auch für die Verschlüsselung der SSD verwendet.

Dadurch können wir garantieren, dass das EDGE Device nicht manipuliert wird oder Daten ausgelesen werden. Wird z.B. die SSD ausgetauscht, fährt das System nicht mehr hoch.

Hinzu kommt, dass sich das EDGE Device nach einer bestimmten Anzahl an Attacken sperrt, wodurch auch hier ein möglicher Angriff unterbunden wird.

Schnittstellen

Beim Design des EDGE Devices wurde darauf geachtet, dass die Anzahl der Hardware-Schnittstellen so weit wie möglich minimiert werden. Zusätzlich sind vorhandene Schnittstellen stark eingeschränkt. Somit hat das EDGE Device z.B. zwar einen USB-Port, es kann jedoch kein USB-Stick angeschlossen und verwendet werden. Des Weiteren ist auch das BIOS verschlüsselt und kann somit nicht verändert werden.

Applikationen

Nur die wichtigsten Services, wie z.B. der Update-Mechanismus des EDGE Devices laufen als Komponenten direkt am Debian Betriebssystem. Alle anderen Anwendungen, laufen als Mikroservices in abgesicherten Docker-Containern. Die einzelnen Docker-Container werden nur gestartet, wenn die darin laufenden Services auch benötigt werden. Außerdem können nur Container auf das EDGE Device geladen werden, die explizit von ENGEL abgenommen, getestet und signiert wurden. Details zu den Prüfungen der Services in den Docker Containern finden Sie im Kapitel „Dependency Check für Docker Container“.

Durch die Verwendung von Docker können wir sicherstellen, dass ein eventuell infizierter oder übernommener Container trotzdem keinen Zugriff auf das Betriebssystem oder andere Container hat. Für die Kommunikation zwischen Containern gibt es eingeschränkte definierte APIs.

Zugriff auf das EDGE Device

Es gibt auf dem EDGE Device keinen Benutzer, der sich z.B. auf der bash anmelden kann. Somit kann lokal nicht direkt auf das Betriebssystem des EDGE Devices zugegriffen werden. Das EDGE Device kann über einen Web-Assistenten, der nur direkt auf der LAN-Schnittstelle SUPPORT verfügbar ist, mit einer IP-Adresse konfiguriert und ongeboardet werden. Alle anderen Zugriffe auf das EDGE Device laufen über Clients, die einem bestimmten gekauften ENGEL Service dienen. Diese Clients haben wiederum keinen vollen Zugriff auf das EDGE Device sondern laufen in einem Docker Container.

Die Konfiguration des EDGE Devices (mit Ausnahme der Netzwerkkonfiguration) kann somit ausschließlich remote z.B. im ENGEL Kundenportal durchgeführt werden. Dazu benötigt das EDGE Device eine Verbindung zu den ENGEL-Endpunkten. Dadurch können wir wiederum sicherstellen, dass nur ein echtes ENGEL EDGE Device Updates und Konfigurationen von ENGEL erhält.

EDGE Device Verbindung zu ENGEL

Bei der Installation des EDGE Devices bei unserem Hersteller wird jedes EDGE Device mit einem eindeutigen Hardware-Zertifikat ausgestattet.

Damit das EDGE Device eine Verbindung zu den ENGEL Endpunkten aufbauen kann, muss es initial einmal ongeboardet werden. Dazu muss im Kundenportal für das erhaltene EDGE Device mithilfe der Kombination aus Seriennummer und der Prüfnummer, die am EDGE Device aufgeklebt ist, ein Token angefordert werden. Dieser Token muss anschließend im Webassistenten, welcher nur über die LAN-Schnittstelle SUPPORT am EDGE Device erreichbar ist, nach der Konfiguration der IP-Adresse eingegeben werden und ist nur für ein Onboarding dieses einen Gerätes gültig. Direkt bei der Eingabe versucht das EDGE Device eine Verbindung zu e3.engelglobal.com auf Port 443 aufzubauen. Der Server überprüft dabei, ob die Kombination aus Hardware-Zertifikat und Token übereinstimmt. Mit diesem Mechanismus wird kontrolliert, ob das EDGE Device während des Versandes vom Lieferanten zum Kunden nicht manipuliert oder ausgetauscht wurde.

Wenn die Kombination aus Hardware-Zertifikat und Token übereinstimmt, bekommt das EDGE Device ein Client-Zertifikat, welches für die zukünftige Kommunikation verwendet wird. Aus diesem Grund darf für die Kommunikation des EDGE Devices zu den ENGEL Endpunkten keine Packet Inspection durchgeführt

werden. Falls eine Packet Inspection durchgeführt wird, nimmt der e3.engelglobal.com die Verbindung des EDGE Devices nicht an.

Sollte das EDGE Device einmal mehrere Monate keine Verbindung zu e3.engelglobal.com herstellen können, läuft das Client-Zertifikat ab und das Onboarding des EDGE Devices muss nochmals durchgeführt werden.

Das EDGE Device baut keine stehenden Verbindungen auf, sondern setzt je nach Anwendungsfall entweder auf Polling oder erneuert die Verbindungen regelmäßig. Damit ist sichergestellt, dass kein Schlüssel zu lange verwendet wird.

Prozess-Sicherheit

Sicherheit vor Hardware-Austausch

Das EDGE Device wird direkt beim Hardware-Lieferanten installiert. Dabei bekommt das EDGE Device auch ein eindeutiges Hardware-Zertifikat, welches am EDGE Device abgelegt wird. Zusätzlich wird dieses Hardware-Zertifikat bei ENGEL abgelegt, um später einen Vergleich durchführen zu können.

Beim Onboarding des EDGE Devices im Kundenportal muss zu der vorhandenen EDGE Device Seriennummer die Prüfsumme eingegeben werden, die auf dem Gerät aufgeklebt ist. Durch die Eingabe der Prüfsumme erhält man einen Token, welcher nur für dieses eine EDGE Device für ein erfolgreiches Onboarding gültig ist.

Der Token muss anschließend im Webassistenten des EDGE Devices nach der Konfiguration der IP-Adresse eingegeben werden. Direkt bei der Eingabe versucht das EDGE Device eine Verbindung zu e3.engelglobal.com aufzubauen. Dabei prüft der e3-Server, ob die Kombination des Hardware-Zertifikats mit dem Token gültig ist. Ist dies der Fall, bekommt das EDGE Device ein Client-Zertifikat für die weitere Kommunikation ausgestellt. Dieses Client-Zertifikat wird regelmäßig automatisiert erneuert, wenn das EDGE Device eine Verbindung zu den ENGEL Endpunkten aufbauen kann.

Durch den Einsatz des TPM-Chips und der SSD-Verschlüsselung können wir sicherstellen, dass das EDGE Device nicht geklont oder manipuliert wurde. Durch den Einsatz des Hardware-Zertifikats gemeinsam mit dem Onboarding-Prozess können wir ebenfalls ausschließen, dass sich ein Angreifer als EDGE Device ausgibt oder versucht ein EDGE Device nachzubauen.

Updates
Updates können nur remote durchgeführt werden. Dafür benötigt das EDGE Device eine Verbindung zu e3.engelglobal.com. Über diesen Mechanismus kann das EDGE Device jegliche Art von Updates (Betriebssystem, Komponenten, Docker Container, etc.) beziehen. Das EDGE Device bekommt jedoch nur Updates, die auch von ENGEL getestet und freigegeben wurden.

Betriebssystem und Komponenten
Updates für das Debian Betriebssystem und Komponenten werden regelmäßig durchgeführt. Dabei werden auch größere Upgrades remote durchgeführt. Alle Updates werden vorher bei ENGEL mehrfach getestet und geprüft, bevor sie anschließend in Wellen an alle EDGE Devices ausgerollt werden.

Docker Container
Wie auch beim Betriebssystem gibt es für die Services, die als Docker Container laufen, regelmäßige Updates. Diese Updates werden ebenfalls vor dem Ausrollen in Wellen bei ENGEL geprüft und getestet. Bevor eine neue Version eines Docker Containers ausgerollt wird, muss dieser signiert werden. Das EDGE Device kann ausschließlich signierte Container herunterladen und starten. Dadurch können wir sicherstellen, dass keine Container am EDGE Device gestartet werden, die nicht von ENGEL freigegeben wurden.

Sicherheit im Entwicklungsprozess

Dependency Check
Um möglichst schnell auf auftretende Schwachstellen reagieren zu können, verwenden wir in unserem Entwicklungsprozess automatisierte Dependency Checks. Dabei unterscheiden wir zwischen selbst entwickelter Software und gelieferter Software. Eine gelieferte Software ist z.B. das Debian Betriebssystem oder Services (Docker Container) von Applikationen, die zugekauft wurden, wie e-connect.24.
Wird eine Abhängigkeit mit einer Schwachstelle im Produktivsystem entdeckt, wird die betroffene Software upgedatet. Der Zeitraum der Auslieferung des Updates hängt dabei vom CVS der Schwachstelle ab.

Selbst entwickelte Software

Bei jeglicher Software, die von ENGEL entwickelt wird und am EDGE Device läuft, wird in der Pipeline ein Dependency Check durchgeführt. Somit können wir garantieren, dass keine Software ausgeliefert wird, bei der bei der Auslieferung bereits eine Schwachstelle bekannt ist.
Damit produktive Software nicht nur bei Anpassungen, sondern regelmäßig geprüft wird, läuft diese Pipeline wöchentlich durch.

Gelieferte Software

Um auch das Betriebssystem und zugekaufte Docker Container auf mögliche Schwachstellen mit dem Dependency Check zu prüfen, gibt es in unserem Testaufbau zwei EDGE Devices, auf denen alle Docker Container laufen, die ENGEL im Einsatz hat. Ein EDGE Device stellt dabei den aktuellen Produktivzustand und ein Gerät den Entwicklungszustand dar. Diese Geräte werden nun wöchentlich von einem zentralen Service der ENGEL IT komplett durchgescannt und auf mögliche Abhängigkeiten mit bekannten Schwachstellen geprüft. Dabei werden sowohl das Betriebssystem mit allen Komponenten als auch die laufenden Docker Container geprüft.

Penetration Test

In größeren Zeitabständen wird für das EDGE Device und die ENGEL Endpunkt von einer unabhängigen Firma ein Penetration Test durchgeführt. Die Ergebnisse laufen anschließend wieder in die Entwicklungen des EDGE Devices mit ein.