Vorgaben für Fronius-externe IT-Administratoren

Externe Dienstleister haben bei Tätigkeiten an Fronius-IT-Assets (z.B. IT-Systemen) folgenden Pflichten einzuhalten:

- Alle Tätigkeiten haben sich strikt innerhalb des vereinbarten Arbeitsauftrags und konkretisierenden Vorgaben von Fronius zu halten.
- Die Abnahme der Leistung erfolgt durch Fronius.
- Die durchgeführten Tätigkeiten sind schriftlich zu dokumentieren.
- Ein Account- oder Passwort-Sharing ist nicht gestattet – jeder Mitarbeiter des externen Dienstleisters hat ausschließlich einen ihm persönlich zugewiesenen Fronius-Account zu benutzen. Damit wird die Nachvollziehbarkeit der durchgeführten Tätigkeiten gewährleistet.
- Privilegierte Accounts bzw. Sessions dürfen nur für die Dauer der administrativen Tätigkeit genutzt werden und müssen umgehend nach Beendigung der Tätigkeit gesperrt werden.

Arbeitsumgebung des externen IT-Administrators

- Firmenfremde/Nicht-Fronius Geräte dürfen nicht mit dem Fronius-Netzwerk (ausgenommen Gäste-WLAN oder dedizierte VPN-Verbindung) verbunden werden.
- Bei Remote-Zugriff via VPN ist ausschließlich der, von Fronius freigegebene VPN-Client, zu verwenden.
- Die Arbeitsumgebung des externen IT-Administrators muss dem Stand der Technik hinsichtlich IT-Security genügen (aktuelles Betriebssystem mit aktuellen Patch-Stand, aktueller Virenscanner...).

Härtung von IT-Systemen

Fronius-IT-Systeme sind entsprechend zu härten, um das Risiko einer Ausnutzung möglicher Angriffsvektoren oder IT-Schwachstellen zu reduzieren.

Die Härtung eines IT-Systems ist insb. durch folgende Maßnahmen sicherzustellen:

- Nicht benötigte Dienste müssen deaktiviert werden
- Nicht benötigte Benutzerkonten müssen deaktiviert werden
- Herstellerpasswörter (Default-Passwörter) müssen geändert werden
- Zusätzliche Software oder Software-Funktionalitäten dürfen nur installiert werden, wenn sie für den Betrieb des Systems notwendig sind
- Etwaige Herstellerangaben zur Härtung eines Systems müssen eingehalten werden

Meldepflicht bei Informationssicherheitsvorfällen

- Erlangt der externe IT-Administrator Kenntnis über einen Informationssicherheitsvorfall (z.B. Infektion mit Schadsoftware) oder ist er hiervon selbst betroffen, ist eine umgehende Meldung an den jeweiligen Fronius-Ansprechpartner durchzuführen.