Benutzerzugriffskontrolle & menschliches Fehlverhalten

Benutzerzugriffskontrolle

Ziel der Benutzerugriffskontrolle:

Im OT-Kontext wird meistens zwischen drei Arten von Benutzern unterschieden:

- Menschliche Benutzer
- Geräte
- Software

Die Benutzerzugriffskontrolle sorgt dafür, dass allen Arten von Benutzern Konten zugewiesen werden, die den Zugriff auf das IACS (Industrial Automation & Control Systems) ermöglichen und aber auch kontrollieren.

Benutzeridentität:

Ein Konto stellt die digitale Repräsentation des Benutzers dar und durch Identifikatoren werden Benutzer mit Authentifikatoren und Konten verbunden. Beispielsweise geben Passwörter Benutzern die Erlaubnis, das zugehörige Konto zu verwenden.

Zugriffsrechte:

Einem Benutzerkonto kann eine oder mehrere Rollen haben, die eine Menge von Einzel-Rechten anhand der vorgesehenen Aufgaben der Rolle zusammenfassen.

Deaktivieren und Entfernen der Benutzeridentität:

Falls ein Benutzer den Zugriff auf das System oder ein Teil davon nicht mehr benötigt, sollte der Zugriff des Benutzers entfernt werden. Für den Fall, dass der Benutzer nur für einen vorübergehenden Zeitraum einen Zugriff nicht mehr benötigt, sollte der Zugriff für diesen Zeitraum deaktiviert werden.

Prinzip der geringsten Rechte:

Benutzer haben bestimmte Aufgaben, die sie während ihrer Tätigkeit erledigen sollen. Deshalb ist es sinnvoll und notwendig, nur die Zugriffsrechte, die zur Erfüllung der zugewiesenen Aufgaben vorgesehen sind, zu gewähren. Dadurch wird die Sicherheit des Unternehmens gefördert, in dem u. a. den Schutz der Daten, Fehlertoleranz verbessert.

Zwei-Faktor-Authentifizierung:

Die Multifaktor-Authentifizierung setzt sich aus einer Kombination von Authentifizierungsarten zusammen, die der Benutzer verwendet, um Zugriff auf sein Konto zu erhalten.
Beispiele für Authentifizierungsarten:

- Passwort
- PIN
- Smartcard
- Sicherheits-Token
- Fingerabdruck

Sichere Passwörter:

Passwörter sollen komplex sein, um die Kompromittierung und Verwendung von kompromittierter Passwörter zu erschweren. Außerdem sollten Passwörter niemals weitergegeben werden.

Anmeldeaktivitäten:

Die historischen Anmeldeinformationen bieten den Benutzern an, ausführliche Anmeldeinformationen zu ihrem Konto einzusehen. Dadurch können Benutzer an der Sicherheit des Systems teilhaben, in dem sie bei Unregelmäßigkeiten die zuständige Abteilung darüber informieren.

Menschliches Fehlverhalten

Verstöße gegen die OT-Richtlinien können ein großes Risiko für die Sicherheit des Unternehmens darstellen und dadurch können auch externe Angriffe ermöglicht werden.

Deshalb ist es immer wichtig, die OT-Richtlinien bzw. auch die IT-Richtlinien zu beachten, beispielsweise:

- (Computer-)Arbeitsplatz auch bei kurzer Abwesenheit sperren
- Zugangsdaten nicht weitergeben
- Sicherer Umgang mit Unternehmensdaten und Dokumenten
- Bei Unklarheiten immer bei der zuständigen Abteilung fragen

Dieses Dokument orientiert sich an der IEC-62443-2-1 Norm, insbesondere die Komponente SPE6 - Benutzerzugriffskontrolle