ABB ABILITY™ CYBER SECURITY SERVICES

ABB Ability™ System Hardening
Systembarrieren stärken

Das ABB Ability™ System Hardening umfasst je nach Anforderung verschiedene Serviceleistungen:

- System Hardening
- Secure Datatransfer
- Network Security
- OPC Secure Gateway
- Awareness Training

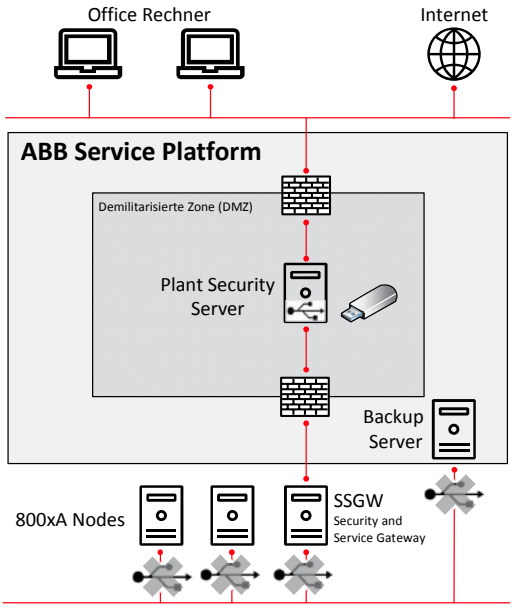
PROTECT

Die folgenden Schutzmaßnahmen erschweren den unerlaubten Zugriff auf Ihr System. Es werden sowohl technische Lösungen als auch Sensibilisierungsmaßnahmen für Ihre Mitarbeiter angeboten.

System Hardening
System Hardening ist eine Basismaßnahme um grundlegende Sicherheitsstandards zu erfüllen. Dies umfasst:

- Verriegeln nicht benutzter Ports
- Entfernen oder Deaktivieren unnötiger Software und Dienste
- User/Password Management
- Überprüfen und Anpassen von Gruppenrichtlinien

Secure Datatransfer
Der Datenaustausch mit dem Automatisierungssystem erfolgt ausschließlich über den Plant Security Server. Es werden alle USB Ports und externen Laufwerke des Leitsystems verriegelt. Auf dem Plant Security Server werden die Daten überprüft und zum Transfer bereitgestellt. Diese Quarantäne-Rechner Funktionalität erhöht ebenfalls die Datensicherheit bei Remotesitzungen über Fernwartungszugänge. Der Zugriff auf die Daten ist trotz höchster Sicherheit benutzerfreundlich von jedem Rechner aus gewährleistet.

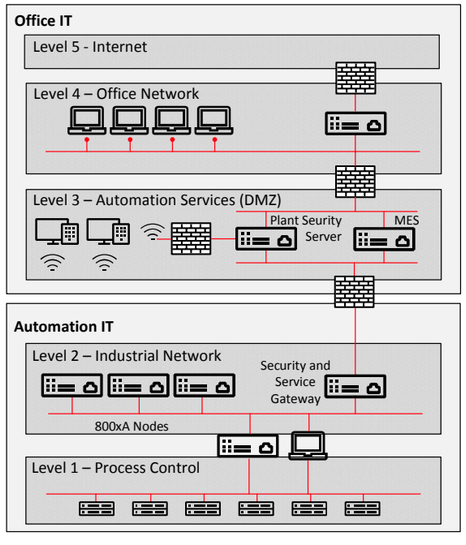


Network Security
Schützen Sie den Datenverkehr Ihres Systems. Das Netzwerk als zentrale Komponente des Leitsystems sollte grundlegende Funktionalitäten bereitstellen, die das System vor unbefugtem Zugriff von außen schützen. ABB liefert individuelle Lösungen, die dem Stand der Technik in der Cybersicherheit entsprechen.

Die Absicherung von Netzübergängen ist einer der entscheidenden Faktoren für eine wirksame Abwehr von Angriffen aus dem Internet oder über das Intranet. Alle externen Schnittstellen zum Automatisierungssystem werden identifiziert und auf Notwendigkeit und Sicherheit überprüft. Der Datenverkehr kann durch eine Datenflusskontrolle, beispielsweise eine Firewall, auf das betriebliche notwendige Maß reglementiert und überwacht werden.

Standardisierte Netzwerkstrukturen erhöhen die Sicherheit. Das Netzwerk des Automatisierungssystems sollte aus mehreren Netzsegmenten, wie zum Beispiel Bedien- und Prozessstationsebene, mit unterschiedlichen, individuellen Schutzbedarfe bestehen. Durch den Aufbau einer demilitarisierten Zone (DMZ) werden Netzwerke wirksam getrennt.

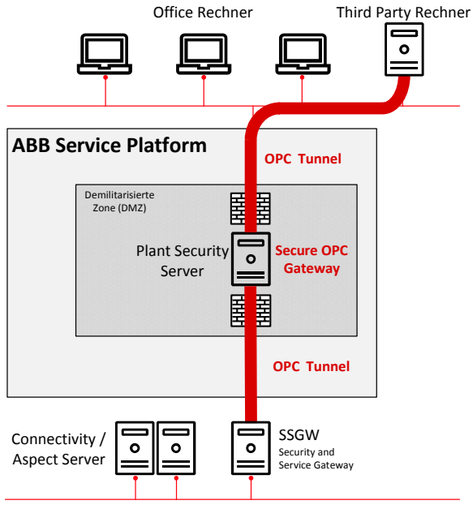
Basismaßnahmen im Bereich des Netzwerks:
- Netzwerksegmentierung durch VLANs
- Erweiterte Netzwerksegmentierung durch den Einsatz von Firewalls
- Implementieren einer demilitarisierten Zone (DMZ)
- Einhaltung der ABB-Passwortrichtlinien für Netzwerkgeräte
- Einschränkung der Zugriffe
- Abschalten nicht benutzter Netzwerkports
- Erhöhung der physischen Sicherheit
- Sicherung von Switch-Konfigurationen



Secure OPC Gateway
Sichere OPC Server/ -Client Kommunikation. IT Netzwerke werden in Sicherheitsstufen unterteilt, um besonders schützenswerte oder kritische Daten vor ungewollten Zugriffen zu bewahren. Die Schnittstelle und klare Trennung solcher Sicherheitsstufen bedarf hierbei einer besonderen Aufmerksamkeit, da diese Punkte eine Einstiegsmöglichkeit für Angreifer bieten.

In der klassischen OPC DA/AE Kommunikation ist die Segmentierung durch Firewalls und somit auch die Trennung durch Sicherheitsstufen sehr schwierig. Mit Secure OPC Gateway wird dieser historische Mangel behoben. Die Kommunikation zwischen verschiedenen Sicherheitsstufen läuft kontrolliert ab und ein Zugriff von einem geringeren Sicherheitslevel zu einem höheren, wird deutlich erschwert.

Optimieren Sie Ihre Prozesse mit modernen Manufacturing Execution System (MES) Systemen und transportieren Sie diese Informationen kontrolliert vom Leitsystem in Ihr MES Netzwerk.



Awareness Training
Das Sensibilisieren aller in einer Anlage beschäftigten Mitarbeiter ist eine einfache, sehr effektive Möglichkeit, auf die gefährlichsten Schwachstellen, Bedrohungen und Gefahren aufmerksam zu machen. Das erworbene grundlegende Verständnis für das Thema Cyber Security hilft Angriffe zu vermeiden.

Das Cyber Security Awareness Training ist für Bediener, Instandhalter, technische Verantwortliche und Anlagenverantwortliche ausgelegt. Um diesen unterschiedlichen Personenkreisen gerecht zu werden, ist dieses Eintagestraining zielgruppengerecht in zwei Trainingseinheiten unterteilt. ABB University bietet hierzu das Awareness Training D467 als vor Ort Training an.

ABB Automation GmbH
Service Control
Oberhausener Strasse 33
40472 Ratingen, Deutschland
Kundencenter Service: +49 180 5 222 580*
Fax: +49 621 38 193 129 031
automation.service@de.abb.com

www.abb.de/
industrieautomation

* 14 Cent/Minute aus dem deutschen Festnetz, max. 42 Cent/Minute aus dem Mobilfunknetz

3BDD017469 REV B 05.2019