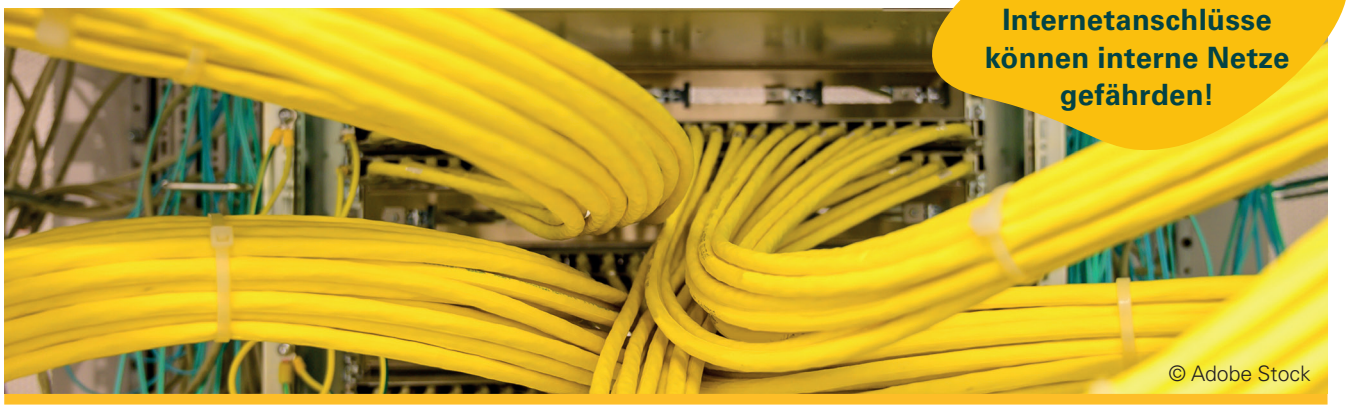
CSBW
CYBER
SICHERHEITS
AGENTUR
BADEN-WÜRTTEMBERG

Netzkopplung und Fernzugriffe

Eine Netzkopplung liegt vor, wenn in einer Einrichtung ein Internetanschluss parallel zu einem internen Netz betrieben wird und die Netze dadurch direkt oder indirekt miteinander verbunden sind. Wenn diese Übergänge nicht ausreichend abgesichert sind, entstehen Einfallstore für Schadsoftware. Fernzugriffe ermöglichen, unabhängig vom Standort einer Institution, den Zugriff auf Daten und Anwendungen. Nicht richtig abgesichert, bergen diese Risiken.



Häufige Probleme:

- Die eigene Netz-Infrastruktur ist unbekannt, nicht dokumentiert oder hat unbekannte Netzübergänge.
- Netzübergänge sind nicht ausreichend mit Sicherheits-Gateways abgesichert.
- Fernwartungs-Zugänge sind nicht ausreichend gesichert, z. B. ohne strenge Passwort-Richtlinien oder Zwei-Faktor-Authentisierung.
- Schutzprogramme gegen Schadsoftware sind als alleinige technische Absicherung nicht ausreichend.
- Eine Netzkopplung kann auch unwissentlich durch IT-Systeme des Gebäudes, DSL-Modems oder IoT-Geräte erfolgen, z.B. durch Heizungen, Photovoltaikanlagen, Aufzüge und Zutrittskontrollsysteme.
- Auch Gäste-WLANs und herstellerspezifische Fernwartungszugänge können Einfallstore für Angriffe sein.

Netzkopplung und Fernzugriffe

Empfehlungen für Fernzugriffe[1]

Architektur:

- Einheitliche Architekturen verwenden.
- Fernwartungskomponenten in vorgelagerte Zonen setzen, z.B. in eine eigene DMZ (Demilitarized Zone, speziell kontrolliertes und abgesichertes Netzwerk).
- Fernwartungszugriffe feingranular pro IP und Port festlegen.
- Verbindungsaufbau nur aus der Institution heraus und ausschließlich für Fernwartungszwecke nutzen.
- Mit dem Internet verbundene Systeme müssen stets aktuell gepatcht sein.

Sichere Kommunikation:

- Sichere Protokolle verwenden, z.B. IPSec, SSH, SSL/TLS.
- Starke Verschlüsselungsverfahren verwenden, z.B. AES-192.

Authentisierungsmechanismen:

- Nur eine nutzende Person pro Account erlauben.
- Zwei-Faktor-Authentisierung einsetzen.
- Ausreichend strenge Passwortrichtlinien festlegen und etablieren.
- Mechanismen zur Detektion von Angriffen einrichten.

Organisatorische Anforderungen:

- Formale Risikoanalyse für die Fernwartungslösung durchführen.
- Nur unbedingt notwendige Fernzugriffsmöglichkeiten erlauben.
- Remote-Zugänge nur bei Bedarf freigeben.
- Fernwartungszugriffe regelmäßig prüfen.
- Definierten Patch-Prozess etablieren.
- Protokollierungsfunktionen nutzen, z.B. um fehlgeschlagene Login-Versuche festzuhalten.

Quellen und weiterführende Literatur:

[1] Fernwartung im industriellen Umfeld, BSI / Allianz für Cybersicherheit: https://www.allianz-fuer-cybersicherheit.de/SharedDocs/Downloads/Webs/ACS/DE/BSI-CS/BSI-CS_108.pdf

Sicherer Fernzugriff auf das interne Netz (ISi-Fern), BSI-Leitlinie zur Internet-Sicherheit (ISi-L): https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Internetsicherheit/isi_fern_leitlinie_pdf.pdf

Grundregeln zur Absicherung von Fernwartungszugängen, BSI / Allianz für Cybersicherheit: https://www.allianz-fuer-cybersicherheit.de/SharedDocs/Downloads/Webs/ACS/DE/BSI-CS/BSI-CS_054.html

CSBW
CYBER SICHERHEITS AGENTUR
BADEN-WÜRTTEMBERG

Weitere Factsheets und Informationen unter:
www.cybersicherheit-bw.de

CSBW Prävention
Kontakt: schulungen@cybersicherheit.bwl.de
Stand: 05.2023