

Cyber-Sicherheitskonzept der CAVITÄT

Informationssicherheit als Grundlage moderner Produktions- und Unternehmensprozesse

Die zunehmende Vernetzung von Produktionsanlagen, Maschinen und IT-Systemen stellt Unternehmen vor stetig wachsende Herausforderungen im Bereich der Cyber-Sicherheit. Gleichzeitig steigen die Anforderungen an Verfügbarkeit, Integrität und Vertraulichkeit von Daten sowie an die Stabilität technischer Prozesse.

Vor diesem Hintergrund verfolgt die CAVITÄT ein umfassendes und mehrschichtiges Cyber-Sicherheitskonzept. Ziel ist es, Unternehmensdaten, Produktionsanlagen und IT-Systeme nachhaltig vor Cyberangriffen, Schadsoftware und unbefugten Zugriffen zu schützen und gleichzeitig einen stabilen, sicheren und effizienten Betrieb zu gewährleisten.

Das Sicherheitskonzept basiert auf dem Prinzip der „Defense in Depth“ – einer mehrstufigen Verteidigungsstrategie, bei der mehrere Sicherheitsmechanismen ineinandergreifen und sich gegenseitig ergänzen.

1. Netzwerksicherheit und Perimeterschutz

Die Absicherung der IT-Infrastruktur erfolgt durch eine zentrale Firewall-Architektur, die den gesamten Netzwerkverkehr kontrolliert, filtert und überwacht.

Zu den umgesetzten Maßnahmen gehören:

- Einsatz einer leistungsfähigen Firewall zur Steuerung aller Netzwerkverbindungen
- Einsatz von White- und Backlists zur gezielten Freigabe und Sperrung von Kommunikationswegen
- Kontrolle und Protokollierung sämtlicher Netzwerkzugriffe
- Einschränkung und Deaktivierung nicht benötigter Ports, Dienste und Protokolle
- Kontinuierliche Überwachung des Netzwerkverkehrs zur Erkennung verdächtiger Aktivitäten

Durch diese Maßnahmen wird die externe Angriffsfläche erheblich reduziert und unautorisierte Zugriffe werden frühzeitig erkannt und verhindert.

2. Endpoint Protection und Schadsoftwareabwehr

Zum Schutz aller Server- und Arbeitsplatzsysteme setzt die CAVITÄT eine zentral verwaltete Endpoint-Security-Lösung ein.

Diese gewährleistet:

- Echtzeitschutz vor Viren, Trojanern, Ransomware und weiterer Schadsoftware
- Kontinuierliche Analyse von System- und Benutzerverhalten
- Automatische Aktualisierung von Sicherheitsinformationen
- Zentrale Verwaltung und Überwachung aller Endpunkte
- Schnelle Erkennung und Reaktion auf sicherheitsrelevante Ereignisse

Die Kombination aus präventiven und Detektiven Schutzmechanismen sorgt für eine hohe Widerstandsfähigkeit gegenüber aktuellen Cyberbedrohungen.

3. Netzwerksegmentierung und Schutz kritischer Systeme

Ein wesentlicher Bestandteil des Sicherheitskonzepts ist die konsequente Trennung unterschiedlicher Netzwerkbereiche.

Hierzu setzt die CAVITÄT auf eine strukturierte VLAN-Segmentierung, durch die:

- Produktions-, Verwaltungs- und IT-Netzwerke voneinander getrennt werden
- Maschinen und Anlagen in isolierte Netzwerkzonen eingebunden sind
- kritische Systeme vom direkten Internetzugang ausgeschlossen werden
- Bewegungen potenzieller Schadsoftware innerhalb des Netzwerks eingeschränkt werden

Diese Architektur verhindert, dass sich Sicherheitsvorfälle unkontrolliert im gesamten Netzwerk ausbreiten können.

4. Datensicherung und Notfallmanagement

Zur Sicherstellung der Geschäftskontinuität verfügt die CAVITÄT über ein strukturiertes Backup- und Wiederherstellungskonzept.

Dieses umfasst:

- regelmäßige, automatisierte Datensicherungen
- getrennte bzw. besonders geschützte Backup-Strukturen
- unveränderbare bzw. geschützte Sicherungskopien zur Abwehr von Manipulation (z. B. durch Ransomware)
- regelmäßige Tests der Wiederherstellbarkeit von Daten
- definierte Notfall- und Wiederanlaufpläne für Systemausfälle oder Cyberangriffe

Damit wird sichergestellt, dass der Betrieb auch im Ernstfall schnell und kontrolliert wieder aufgenommen werden kann.

5. Systemhärtung und Patch-Management

Alle Server, Clients und mobilen Endgeräte werden nach aktuellen Sicherheitsstandards betrieben und kontinuierlich gepflegt.

Zu den Maßnahmen zählen:

- regelmäßige Installation von Sicherheitsupdates und Patches
- Entfernung nicht benötigter Softwarekomponenten
- Deaktivierung überflüssiger Dienste und Funktionen
- konsequente Systemhärtung zur Reduzierung von Angriffsflächen

6. Kontrolle externer Zugriffe und Fernwartung

Externe Zugriffe auf Systeme der CAVITÄT werden streng kontrolliert und dokumentiert.

Dabei gilt:

- Fernwartungszugriffe sind nur in einem definierten Rahmen möglich
- alle externen Zugriffe werden vollständig protokolliert
- Kommunikationsverbindungen zwischen Maschinen und Systemen sind dokumentiert und nachvollziehbar
- Zugriffe erfolgen ausschließlich über freigegebene und kontrollierte Wege

So wird sichergestellt, dass externe Eingriffe jederzeit transparent und kontrollierbar bleiben.

7. Organisatorische Sicherheitsmaßnahmen

Neben technischen Schutzmechanismen sind organisatorische Maßnahmen ein zentraler Bestandteil des Sicherheitskonzepts.

Die CAVITÄT setzt hierzu auf:

- verbindliche Richtlinien zur Informationssicherheit für alle Mitarbeiter
- Schulungen und Awareness-Maßnahmen zur Cyber-Sicherheit
- klar definierte Verantwortlichkeiten im Bereich IT- und Informationssicherheit
- strukturierte Prozesse zum Umgang mit Sicherheitsvorfällen (Incident Response)