# IT-SECURITY

## FlowChief GmbH

## Sicherheitsrichtlinien innerhalb der Softwareentwicklung

Die Entwicklung zeitgemäßer Software auf dem Stand aktueller Sicherheitsstandards erfordert Disziplin in Form von fest definierten und erprobten Abläufen innerhalb des Unternehmens.

Im Laufe von 20 Jahre Software-Entwicklung etablierten wir zur Sicherstellung und kontinuierlichen Steigerung des Sicherheitsniveaus zahlreiche interne Prozesse, Richtlinien und Abläufe.

- Sensibilisiertes Entwicklerteam, das bereits bei der Implementierung Rücksicht auf potentielle Angriffsvektoren nimmt und dabei aktuelle Kenntnisse und Richtlinien bezüglich sicherer Softwareentwicklung berücksichtigt
- Fundierte Kenntnisse in puncto sichere Webtechnologie basierend auf 20 Jahren Entwicklung und Projektumsetzung
- Stetiger Ausbau unseres Wissens in IT-Security innerhalb unseres Entwicklungs- und Technikteams
- Security-Tests durch das von der Entwicklung unabhängige Testteam
- Aktives Monitoring von CERTS, Technologien und Third-Party-Produkten auf potentielle Schwachstellen (Vulnerability)
- Feste Anlaufstelle für das Melden von Schwachstellen
- Fest definierte interne Abläufe beim Auftreten von Schwachstellen
- Kommunikationskanäle zu Integratoren und Endkunden für die Information über aktuell verfügbare Security Patches
- Bereitstellung von Security Patches (auch für ältere Versionen – im Rahmen unseres Product-Life-Cycle)
- Wir sind Mitglied der vom BSI initiierten Initiative Allianz für Cyber-Sicherheit

## Webtechnik vs. konventionell (proprietär)

Die durchgängige Umsetzung des User Interface in Webtechnologie unterscheidet uns von vielen anderen Produkten. Dabei bevorzugen IT-Verantwortliche webbasierte Lösung. Der Aufwand minimiert sich für die Administration erheblich: Keine Clientupdates, einfachste Einrichtung neuer Clients und ideale Integration in die bestehende IT Infrastruktur sind nur einige Vorteile. Speziell bei der Nutzung von Zonenschutzkonzepten (vertikale, horizontale Segmentierung) sind Netzübergänge auf Basis von Webtechnologie einfacher zu handeln als proprietäre Herstellerlösungen.

Als Fernzugriff auf die Anlage kann z.B. unter Nutzung von DMZs, eine sichere TLS-verschlüsselte Verbindung direkt über den Browser erfolgen. Direkte VPN-Einwahlen in das kritische IT-Netzwerk sind nicht notwendig, können aber als zusätzliche Barriere genutzt werden. Die direkte Einwahl auf Rechner im Netzwerk, z.B. via RDP entfällt vollständig.

Mit einer Vielzahl von Tools kann der Integrator oder Administrator das implementierte System auf die Einhaltung der Sicherheitsvorgaben überprüfen.

**Und:**

**Webtechnik heißt nicht öffentliches Internet – webbasierte Prozessleitsysteme können wie konventionelle Systeme völlig autark vom Internet eingerichtet werden. Bei Bedarf kann ohne viel Aufwand ein sicherer Fernzugriff durch die Administration eingerichtet werden.**

## Sicherheit auf allen Ebenen

Die IT-Grundschutzkataloge unterteilen in 5 Bausteine. Neben der tatsächlichen Anwendung (B5) gibt es auch die Bausteine B1 – Übergreifende Aspekte, B2 – Infrastruktur, B3 – IT-Systeme, B4 – Netze. Ein sicheres Gesamtkonzept ist somit vielschichtig und keinesfalls nur auf Anwendungsebene zu sehen. Allerdings ist es wichtig, dass Anwendungen bereits im Design so konzipiert sind, dass Sie optimal mit Infrastruktur, IT-Systemen, z.B. Betriebssystemen, Netzwerken oder auch Third-Party-Software, zusammenarbeiten.

- Optimales Zusammenspiel mit Sicherheits-Infrastruktur (Firewalls, DMZ, Proxy-Servern und Zellenschutzkonzepten [Defense in Depth]) durch Nutzung von Webtechnologie und Standardprotokollen
- Beschränkung auf einen definierten Zugriffsweg von allen Geräten (Desktop, Mobil usw.) auf einen definierten Webserver (beherrschbar)
- Keine zusätzliche Software für Ferneinwahl notwendig
- Verschlüsselung auf Basis von austauschbaren SSL/TLS Zertifikaten
- Stetige und sofortige Freigabe von Windows Patches inkl. MS SQL Datenbank
- Gehärteter Microsoft IIS
- Kompatibilität zu gängiger Schadsoftwareerkennung (Virenschutz)
- Kompatibilität zu Applikation Whitelisting
- Kompatibilität zu Windows UAC (Benutzerkontensteuerung)
- Schutz vor Denial of Service durch IP/Domain Restriction (IIS Feature)
- Keine hardcodierten Logins für Servicezwecke
- Nutzung von Datenbank Security Features wie Authentifizierung (Konfiguration, Anlagen- und Archivdaten)
- Kompatibel zu SQL Cluster und externen Datenbanken
- Minimalitäts-Prinzip Betriebssystem – Engineering ohne administrative Rechte
- Reine Server-Client-Struktur – Konfiguration und Bedienung ist durchgängig vom Client aus möglich (keine direkte Verbindung mit dem Server)
- Webbasierter Zugriff – keine Ferneinwahl notwendig

Sichere Anlagen fordern ganzheitliche Sicherheitskonzepte und enden keinesfalls auf Applikationsebene! Vielmehr müssen Komponenten wie Betriebssysteme, Netzwerk, gängige Sicherheitskomponenten (Firewall, DMZ usw.) eingerichtet und auch überwacht werden. Schlussendlich ist auch die nötige Sensibilisierung von Anwendern zum Thema unumgänglich. Was nützt eine hochskalierte Sicherheitsinfrastruktur, wenn der Anwender vor Ort über einen USB Stick die vermeintliche Schadsoftware verbreitet?

## Security by Design

Im Rahmen anerkannter Integrationsempfehlungen (z.B.: BSI Grundschutz oder BDEW Whitepaper) setzen wir viele Security-Features direkt in unserer Software um.

### Anwendungssicherheit

- Konsequente Validierung von Eingabedaten
- Keine aktiven Backdoors (hardcodierte Herstellerzugänge)
- Erzwingen eines initialen Passworts-Wechsels
- Schutz vor Brute-Force (Login durch Ausprobieren) – Verdopplung der Zeit zwischen weiteren Authentifizierungsversuchen
- Kennwortrichtlinien (konfigurierbare Stärke, nicht deaktivierbar)
- Verwendung von Standardschnittstellen und -protokollen
- Lauffähig ohne aktive Windows Session (Windows Service)
- Optionale Beschränkung des Logins auf das lokale LAN (pro Benutzer einstellbar)
- Authentifizierungsdaten werden unter Nutzung sicheren Hashings verschlüsselt abgelegt – kein Zurücklesen möglich
- Gekapselter Zugriff über Microsoft IIS (Webserver)

### Benutzerverwaltung

- 2-Faktor-Authentifizierung auf Basis mehrerer Methoden (OATH-TOTP, SMS)
- Active-Directory-Integration (Verwendung der AD-Kennwortverwaltung)
- Rollenbasiertes Berechtigungskonzept (Benutzergruppenunterstützung)
- Feingranulares Rechtemanagement auf Konfiguration, Aktion, Bedienoberfläche mit der Möglichkeit der Beschränkung auf Anlagenteile (volle Mandantenfähigkeit)
- Einfache Passwortänderung durch Benutzer mit vorangestellter Authentifizierung
- Minimalitäts-Prinzip Anwendung – Weitreichende Möglichkeiten zur Einschränkung der Benutzerrechte sowohl auf Datenpunkt- als auch auf Systemfunktionen

### Kryptographie/Verschlüsselung

- OPC UA Sign & Encrypt (Autorisierung & SSL Verschlüsselung X.509 basierte)
- OPC UA Server (SSL Pflicht)
- SMTPS (SMTP über SSL/TLS)
- FTPS (FTP over SSL)
- Unterstützung von S/MIME E-Mail-Verkehr (lesend)

### Sichere Webanwendung

- Konsequente Verschlüsselung via SSL/TLS (austauschbare X.509 Zertifikate)
- Unverschlüsselter Zugriff via http nicht unterstützt

### Überwachung und Protokollierung

- Logging (audit) of security relevant events (accesses, authentication attempts)
- Logging and monitoring data on resource utilization and configuration changes

### Sicherstellung der Verfügbarkeit

- Redundanzlösungen für maximale Verfügbarkeit und Datensicherheit auch während regelmäßiger Patchvorgänge

- Bereitstellung von sicheren und robusten Backup- und Wiederherstellungsprozeduren

## Fernwirktechnik

FlowChief Fernwirktechnik[1] basiert auf Standard SPS-Komponenten. Gängige SPS-Hardware kommuniziert dabei Punkt zu Punkt über verschiedenste Übertragungsmedien mit der Leitstelle. Das Protokoll unterstützt neben einfachen Security Features wie Verschleierung auch eine zertifikatsbasierte Standard-Verschlüsselung via SSL und austauschbare X.509 Zertifikate.

- X.509 zertifikatsbasierte Ende-zu-Ende-Verschlüsselung zwischen SPS und Zentrale (bisher unterstützte Controller bzw. Bibliotheken: Wago)
- TCP/IP basiert und damit voll routingfähig und kompatibel zu gängigen Security-Komponenten Firewalls, DMZs, IDS usw.
- Optimiertes Protokoll zur Datenübertragung inkl. Datenpufferung
- Die Außenstation ist durch das private Provider-Netz vor Zugriffen aus dem Internet geschützt (zusätzlich zur Router-Firewall [Achtung nur Mobilfunk!])
- Authentifizierung und Stationskennung
- Keine Vermittlungsserver – direkte Punkt-zu-Punkt-Verbindung zwischen Außenstation und Zentrale

**Zusätzlich Sicherheitsmaßnahmen (optional)**

- VPN-Tunnelung
- Wegeredundanz
- Redundantes zentrales Leitsystem

## Resümee

Unsere Produkte wurden mittlerweile in mehr als 1.500 Projekten in den Branchen Umwelttechnik, Industrie, Maschinenbau und Energie erfolgreich eingesetzt. Eine Vielzahl dieser Projekte befindet sich in den KRITIS Segmenten oder in Unternehmensnetzwerken mit geltenden IT-Richtlinien. FlowChief bietet viele Security-Features zur Realisierung sicherer Anlagenstrukturen und ist aufgrund seiner Architektur eine passgenaue Lösung für kommunale und industrielle Klein- und Großanlagen.

Haben Sie Fragen zur Ausführung und IT-Sicherheit rund um unsere Softwareprodukte? Wir stehen Ihnen gerne mit unseren Know-how in puncto sicherer Anlagenbetrieb zur Verfügung.

**Sichere IT Infrastruktur ist nur im Kollektiv aus Hersteller – Planer – Systemintegrator und Anwender umsetzbar!**

Sprechen Sie uns an!

**Christian Fink**
Leiter Produktmanagement

Tel.: +49 9129 147 22 32
E-Mail: productmanagement@flowchief.de

[1] FlowChief Prozessleittechnik ist auch zu anderen offenen Fernwirktechniken kompatibel, z.B. FWT auf Basis von IEC 60870-104 oder OPC UA. FlowChief Fernwirktechnik bietet eine offene OPC-Schnittstelle und ist damit auch kompatibel mit Leittechnik anderer Hersteller.