GEUTEBRÜCK

Geutebrück Systemsicherheit

Version: 1.1

Januar 2026

Inhaltsverzeichnis

1 Einleitung: Unser Engagement für Cybersicherheit

Geutebrück liefert fortschrittliche Videolösungen zur Sicherheit und Prozessoptimierung für eine Vielzahl von Kunden, einschließlich Behörden und kritischer Industriebereiche. Diese Kunden haben ein überdurchschnittlich hohes Bedürfnis an sicheren, langlebigen und verlässlichen Systemen. Für unsere Kunden gilt es um jeden Preis zu vermeiden, dass Unbefugte Zugriff auf die Systeme erhalten, sei es, um diese zu sabotieren, zu manipulieren oder Objekte auszuspähen.

Aufgrund der sich rasant entwickelnden Cyber-Bedrohungen hat Geutebrück umfangreiche Maßnahmen eingeführt, um unsere Produkte und Lösungen zu schützen. Unser Sicherheitsansatz ist in jede Phase des Produktlebenszyklus integriert – von der Entwicklung über die Bereitstellung bis hin zur laufenden Wartung. Dieses Dokument gibt einen Überblick über die Sicherheitsmerkmale, Best Practices und Dienstleistungen, die die Integrität und Widerstandsfähigkeit eines Geutebrück-Systems gewährleisten.

2 Secure by Design: Der Entwicklungszyklus

Um eine integrierte und nachhaltige Sicherheit zu erreichen, hat Geutebrück einen **Security Development Lifecycle (SDL)** in unseren Kernentwicklungsprozess integriert. Dieser proaktive Ansatz stellt sicher, dass Sicherheit kein nachträglicher Gedanke, sondern ein fundamentaler Bestandteil unserer Software ist.

Wichtige Bestandteile unseres SDL umfassen:

- **Definition von Sicherheitsanforderungen:** Festlegung strenger Sicherheitskriterien zu Beginn eines jeden Projekts.
- **Durchführung von Bedrohungsanalysen:** Proaktive Identifizierung und Analyse potenzieller Bedrohungen und Schwachstellen in Systemdesigns.
- **Coding Best Practices:** Einhaltung von Industriestandards für die Erstellung von sicherem und robustem Code.
- **Statische und dynamische Code-Analysen:** Einsatz von automatisierten Werkzeugen und manuellen Prozessen (einschließlich Penetrationstests), um potenzielle Schwachstellen im Code aufzudecken.
- **Systematisches Patchmanagement:** Sicherstellung, dass alle Komponenten von Drittanbietern und Betriebssysteme auf dem neuesten Stand der Sicherheitspatches gehalten werden.
- **Sichere Entwicklungsumgebung:** Schutz unserer Entwicklungsprozesse und -werkzeuge durch geeignete Zugriffsberechtigungen und Sicherheitsmaßnahmen.

3 Wichtige Sicherheitsmerkmale

Geutebrück-Systeme sind mit mehreren Sicherheitsebenen ausgestattet, um Daten während der Übertragung und Speicherung zu schützen.

3.1 Verschlüsselte Kommunikation

Sichere Kommunikationskanäle sind unerlässlich, um Abhören und Datenmanipulation zu verhindern.

- **Server- und Client-Kommunikation:** Die Kommunikation zwischen G-Core-Servern, dem Software Asset Management Service (SAM), G-View Clients und G-SIM (Agents und OpCon/ReCon Clients) wird mit dem **Advanced Encryption Standard (AES) mit einer Schlüssellänge mit 256 Bit** verschlüsselt. Der Schlüsselaustausch erfolgt über das sichere **Diffie-Hellman-(DH)**-Verfahren.
- **G-SIM-zu-Client-Kommunikation:** Die Kommunikation zwischen dem G-SIM-Server und seinen Clients wird mittels **Transport Layer Security (TLS)** verschlüsselt, was einen sicheren HTTPS-Kanal bereitstellt.
- **Kamera-Kommunikation:** Für Geutebrück kameras und tief integrierte Drittanbieter-Kameras (z. B. Axis, Bosch) kann die Kommunikation zwischen Kamera und Server mittels **TLS (HTTPS)** verschlüsselt werden. Es wird dringend empfohlen, diese Funktion dort zu nutzen, wo immer sie unterstützt wird. RTSP über HTTPS wird verwendet.
- **System Health Management:** Unsere G-Health-Software unterstützt außerdem HTTPS mit SSL-Zertifikaten für eine sichere Kommunikation.

3.2 Verschlüsselte Datenbanken und Speicherung

- **Proprietäre Videodatenbank:** Unsere Videodatenbank verwendet ein proprietäres Format. Dieses Design schützt inhärent vor Änderungen oder Datenextraktion ohne detailliertes Wissen über die Geutebrück-Datenbankstruktur, da jede unbefugte Änderung zu Datenverlust im entsprechenden Teil der Datenbank führt.
- **Festplattenverschlüsselung:** Für eine zusätzliche Sicherheitsebene für ruhende Daten empfehlen wir die Verwendung von Full-Disk-Verschlüsselungstools wie **Microsoft BitLocker**. BitLocker unterstützt AES-Verschlüsselung (128 und 256 Bit) und kann das gesamte Betriebssystemvolumes, Datenvolumes oder virtuelle Laufwerke sichern.

3.3 Sichere Passwortspeicherung und -übertragung

- **G-Core-Passwörter:** Passwörter in G-Core werden mit dem **Secure Hash Algorithm (SHA−256) mit Salting** gehasht. Die Übertragung von Passwörtern erfolgt doppelt verschlüsselt: Erstens mit **Blowfish** (einer symmetrischen Schlüssel-Blockchiffre) und zweitens mit der Windows-Standard-Passwortverschlüsselung mit Salting, die an die jeweilige Windows-Maschine gebunden ist.

- **G-SIM-Passwörter**: G-SIM-Passwörter werden mit dem Industriestandard-Algorithmus **PBKDF2 mit Salting** gespeichert, der einen starken Schutz gegen Brute-Force-Angriffe bietet.

4 Anleitung zur Systemhärtung

"Härtung" bezeichnet den Prozess der Absicherung eines Systems durch die Reduzierung seiner Angriffsfläche. Obwohl Geutebrück-Systeme bereits mit grundlegenden Sicherheitsmaßnahmen ausgeliefert werden, sollte während der Inbetriebnahme eine weitere Härtung basierend auf den spezifischen Anforderungen des Standorts erfolgen.

4.1 Firmware- und Software-Updates

Halten Sie die Firmware und Software aller Komponenten (Kameras, Server, Clients, Netzwerk-Switches) immer auf dem neuesten Stand. Dies stellt sicher, dass das System durch die neuesten verfügbaren Sicherheitspatches geschützt ist. Überprüfen Sie regelmäßig das Geutebrück Portal für Updates und die Websites der Hersteller für Geräte von Drittanbietern.

4.2 Physische Zugriffskontrolle

Der physische Zugriff auf Server, Workstations, Kameras und Netzwerkperipheriegeräte muss auf autorisiertes Personal beschränkt sein. Dies verhindert Manipulationen wie das unbefugte Anschließen von USB-Geräten, das Entfernen von Festplatten oder das Abziehen von Kabeln.

4.3 Netzwerkkonfiguration und -sicherheit

- **Netzwerksegmentierung:** Das Videoüberwachungsnetzwerk sollte physisch vom Haupt-Unternehmensnetzwerk des Kunden getrennt sein. Wenn eine physische Trennung nicht möglich ist, verwenden Sie **VLANs**, um das Netzwerk logisch zu segmentieren. Eine bewährte Methode ist, Kameras in einem separaten VLAN von den Anzeige-Clients zu betreiben.

- **Firewalls:** Verwenden Sie eine moderne, branchenerprobte Firewall, um das System vor unbefugtem Zugriff zu schützen und das Risiko von Denial-of-Service-(DoS)- oder Distributed-Denial-of-Service-(DDoS)-Angriffen zu minimieren, insbesondere wenn das System mit anderen Netzwerken oder dem Internet verbunden ist.

- **Port-Sicherheit und MAC-Bindung:** Aktivieren Sie auf Netzwerk-Switches Funktionen wie **portbasierte Authentifizierung (IEEE 802.1X)** oder **MAC-Adressbindung**. Dies stellt sicher, dass nur autorisierte Geräte eine Verbindung zu einem Switch-Port herstellen können, und verhindert so unbefugten Netzwerkzugriff.

- **WLAN (Wireless LAN):** Vermeiden Sie nach Möglichkeit den Einsatz von WLAN im sicheren CCTV-Netzwerk aufgrund der erhöhten Sicherheitsrisiken.

- **Fernzugriff:** Der Fernzugriff auf Teile des Systems sollte über ein sicheres **Virtual Private Network (VPN)** unter Verwendung moderner Verschlüsselungs- und Authentifizierungsstandards erfolgen. Setzen Sie niemals ein System ohne Firewall-Schutz direkt dem Internet aus. Wenn eine Portweiterleitung zwingend erforderlich ist, leiten Sie nur die absolut notwendigen Ports weiter und beschränken Sie den Zugriff auf autorisierte Quell-IP-Adressen.

4.4 Geräte- und Anwendungshärtung

- **Nicht genutzte Dienste deaktivieren:** Deaktivieren Sie alle ungenutzten Dienste auf Kameras und Windows-Servern, um die Angriffsfläche zu reduzieren. Dazu gehören Dienste wie SSH, Multicast oder QoS auf Kameras, wenn sie nicht benötigt werden, und Dienste wie SNMP unter Windows, wenn kein Überwachungssystem verwendet wird.

- **Standard-Ports ändern:** Ändern Sie bei Geräten wie Kameras die Standard-Ports für Administration und Streaming, um sie weniger anfällig für automatisierte Angriffe zu machen.

- **SQL-Datenbankzugriff:** Verwenden Sie für Analysen oder Berichte auf der SQL-Datenbank ein Konto mit den minimal erforderlichen Leseberechtigungen. Verwenden Sie für Routineabfragen nicht das sysadmin-Konto.

4.5 Benutzer- und Zugriffsverwaltung

- **Standardpasswörter ändern:** Ändern Sie sofort alle Standard-Administratorkennwörter (Geutebrück-System, Kameras, Switches) in starke, einzigartige Passwörter, die modernen Komplexitätsstandards entsprechen (z. B. OWASP-Passwortrichtlinie). Passwörter sollten regelmäßig geändert werden.

- **Prinzip der geringsten Rechte (Least Privilege):** Konfigurieren Sie die Benutzerrechte so, dass Personen nur Zugriff auf die Funktionen und Daten haben, die für ihre Rolle erforderlich sind. Die Geutebrück-Software ermöglicht eine granulare Steuerung der Benutzerberechtigungen.

- **Windows-Dienstkonten:** Geutebrück-Dienste laufen standardmäßig als "LocalSystem". Wenn ein dediziertes Dienstkonto verwendet wird, stellen Sie sicher, dass es ein sicheres Passwort hat und nur lokale Benutzerrechte besitzt. Ein Domänenadministratorkonto ist nicht erforderlich und wird ausdrücklich nicht empfohlen. Für die LDAP-Synchronisation in G-SIM benötigt das Dienstkonto lediglich Leserechte im Active Directory.

- **Automatische Abmeldung:** Konfigurieren Sie G-SIM so, dass Benutzer nach einer bestimmten Zeit der Inaktivität (z. B. 15-60 Minuten) automatisch abgemeldet werden. Konfigurieren Sie ebenso Windows so, dass die Bildschirmsitzung nach kurzer Inaktivität automatisch gesperrt wird.

- **UAC auf Clients:** Die meisten Geutebrück-Client-Anwendungen benötigen keine Administratorrechte zum Ausführen. Dies trägt dazu bei, die potenziellen Auswirkungen von Malware auf einer Client-Workstation zu begrenzen.

5 Laufendes Sicherheitsmanagement

Sicherheit ist ein kontinuierlicher Prozess, kein einmalige Konfiguration.

5.1 Microsoft Windows Sicherheitsupdates & Patch-Management

Die Installation von Microsoft-Sicherheitsupdates ist von entscheidender Bedeutung. Es ist jedoch unerlässlich, zunächst zu überprüfen, ob diese Updates die Leistung und Stabilität des Geutebrück-Systems nicht beeinträchtigen. Geutebrück bietet einen umfassenden **Patchmanagement-Service** zur Unterstützung von Kunden an, der Folgendes umfasst:

- **Klassifizierung:** Wir prüfen, klassifizieren ("Kritisch", "Wichtig", "Nicht relevant") und dokumentieren alle neuen Microsoft-Updates und geben Empfehlungen zu ihrer Anwendbarkeit auf Geutebrück-Software.

- **Installation:** Basierend auf der Klassifizierung können unsere Experten die Installation genehmigter Patches durchführen, um einen kontrollierten Rollout zu gewährleisten.

- **Test:** Nach der Installation führen wir Funktionstests an der Geutebrück-Software durch, um zu überprüfen, ob der Systembetrieb stabil und performant bleibt.

5.2 Kompatibilität von Antivirensoftware

Die Verwendung einer aktuellen Antivirensoftware wird empfohlen. Um sicherzustellen, dass die Systemleistung nicht beeinträchtigt wird, ist es unerlässlich, die Antivirensoftware mit den folgenden Ausnahmen zu konfigurieren:

- Schließen Sie die Geutebrück-Videodatenbank von Echtzeit- und geplanten Scans aus.

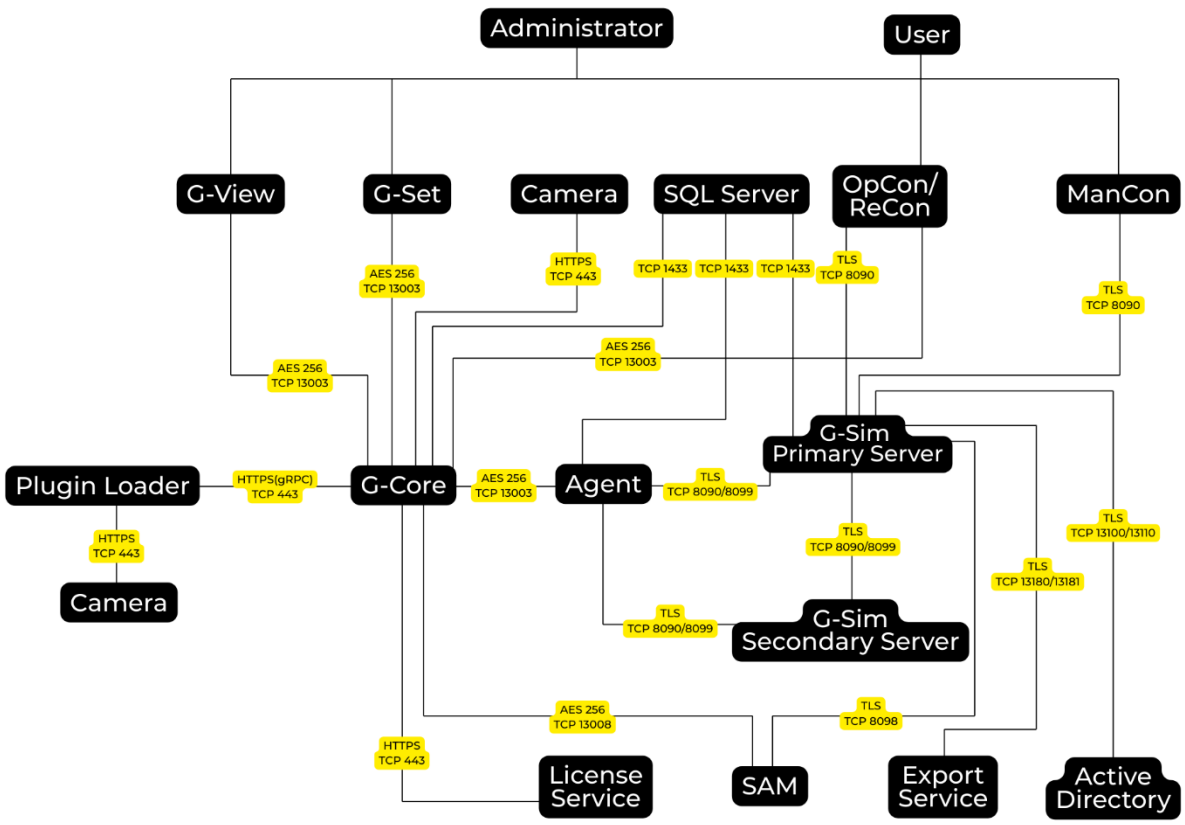
- Fügen Sie Geutebrück-Anwendungsordner und -Bibliotheken zur Whitelist/Ausnahmeliste der Sicherheits-Scans hinzu.

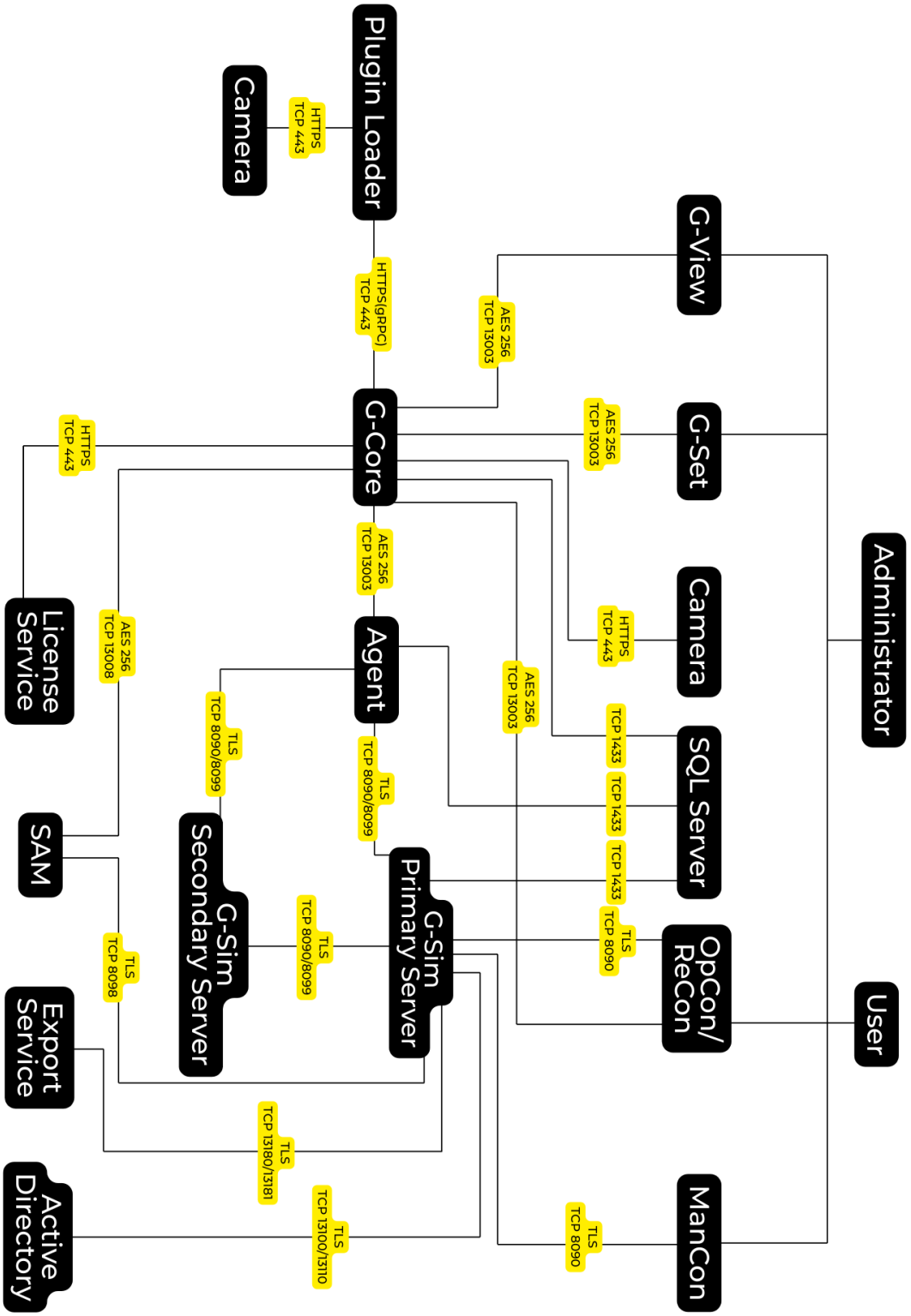
5.3 Schwachstellenmanagement und Support

Geutebrück betreibt eine aktive Marktbeobachtung zur Früherkennung von neuen Bedrohungen und potenziellen Schwachstellen.

- **Schnelle Reaktion:** Erkannte bzw. gemeldete Sicherheitslücken werden in kürzestmöglicher Frist analysiert und entsprechend ihrer Kritikalität behoben.
- **Offene Kommunikation:** Wir pflegen eine offene Informationskultur und informieren Partner und Kunden zeitnah über Feststellungen sowie Lösungsoptionen zu Sicherheitslücken.
- **Central Support:** Unser Central Support steht zur Verfügung, um fachkundige Beratung und Unterstützung bei der Umsetzung von Maßnahmen gegen Sicherheitslücken zu bieten.

6 Kommunikationsschema der Systemkomponenten




Plugin Loader
Camera
HTTPS
TCP 443
HTTPS(gRPC)
TCP 443
G-View
AES 256
TCP 13003
G-Core
G-Set
AES 256
TCP 13003
HTTPS
TCP 443
Administrator
Camera
HTTPS
TCP 443
AES 256
TCP 13003
Agent
AES 256
TCP 13003
License Service
AES 256
TCP 13008
TLS
TCP 8090/8099
TCP 1433
SQL Server
TCP 1433
TCP 1433
TLS
TCP 8090/8099
SAM
G-Sim Secondary Server
G-Sim Primary Server
TLS
TCP 8090/8099
TLS
TCP 8090
OpCon/ ReCon
User
TLS
TCP 8098
Export Service
TLS
TCP 13180/13181
TLS
TCP 13100/13110
Active Directory
TLS
TCP 8090
ManCon