GEUTEBRÜCK

Geutebrück System Security

Versión: 1.1

Enero de 2026

Índice

1 Introducción: Nuestro compromiso con la ciberseguridad

Geutebrück ofrece soluciones avanzadas de vídeo para la seguridad y la optimización de procesos a una amplia gama de clientes, incluidos autoridades públicas y sectores industriales críticos. Estos clientes tienen una demanda excepcionalmente alta de sistemas seguros, duraderos y fiables. Proteger estos sistemas de accesos no autorizados, sabotaje, manipulación o espionaje es de suma importancia.

En respuesta al panorama en rápida evolución de las amenazas cibernéticas, Geutebrück ha implementado medidas integrales para proteger nuestros productos y soluciones. Nuestro enfoque de seguridad está integrado en cada etapa del ciclo de vida del producto, desde el desarrollo hasta el despliegue y el mantenimiento continuo. Este documento ofrece una visión general de las características de seguridad, mejores prácticas y servicios que garantizan la integridad y resiliencia de un sistema Geutebrück.

2 Seguro por diseño: El ciclo de vida del desarrollo

Para lograr una seguridad integrada y sostenible, Geutebrück ha integrado un Ciclo de **Vida del Desarrollo de Seguridad (SDL)** en nuestro proceso central de desarrollo. Este enfoque proactivo garantiza que la seguridad no sea una ocurrencia secundaria, sino un componente fundamental de nuestro software.

Los elementos clave de nuestro SDL incluyen:

- **Definición de requisitos de seguridad:** Establecer criterios estrictos de seguridad desde el inicio de cualquier proyecto.
- **Análisis de amenazas:** Identificación y análisis proactivo de posibles amenazas y vulnerabilidades en el diseño de sistemas.
- **Mejores prácticas de codificación segura:** Cumplir con los estándares del sector para escribir código seguro y robusto.
- **Análisis estático y dinámico de código:** Utilización de herramientas automatizadas y procesos manuales (incluidas pruebas de penetración) para detectar posibles vulnerabilidades en el código.
- **Gestión sistemática de parches:** Garantizar que todos los componentes y sistemas operativos de terceros estén actualizados con los últimos parches de seguridad.
- **Entorno de Desarrollo Seguro:** Proteger nuestros procesos y herramientas de desarrollo con controles de acceso y medidas de seguridad adecuados.

3 Características de seguridad principales

Los sistemas Geutebrück están equipados con múltiples capas de seguridad para proteger los datos en tránsito y en reposo.

3.1 Comunicaciones cifradas

Los canales de comunicación seguros son esenciales para evitar la escucha y la manipulación de datos.

- **Comunicación entre servidor y cliente:** La comunicación entre servidores G-Core, el Servicio de Gestión de Activos de Software (SAM), los clientes G-View y G-SIM (agentes y clientes OpCon/ReCon) se cifra usando el **Estándar Avanzado de Cifrado (AES) con un tamaño de clave de 256** bits. El intercambio de claves se gestiona mediante el método seguro **Diffie-Hellman (DH**).
- **Comunicación G-SIM a Cliente:** La comunicación entre el servidor G-SIM y sus clientes se cifra usando **Transport Layer Security (TLS),** proporcionando un canal HTTPS seguro.
- **Comunicación con cámara:** Para Geutebrück y cámaras de terceros profundamente integradas (por ejemplo, Axis, Bosch), la comunicación entre la cámara y el servidor puede cifrarse usando **TLS (HTTPS).** Se recomienda encarecidamente utilizar esta función cuando sea compatible. Se utiliza RTSP sobre HTTPS.
- **Gestión de la Salud del Sistema:** Nuestro software G-Health también soporta HTTPS con certificados SSL para una comunicación segura.

3.2 Bases de datos y almacenamiento cifrados

- **Base de datos de vídeo propietaria:** Nuestra base de datos de vídeo utiliza un formato propietario. Este diseño protege inherentemente contra modificaciones o extracción de datos sin un conocimiento detallado de la estructura de la base de datos Geutebrück, ya que cualquier cambio no autorizado resulta en corrupción de datos.
- **Cifrado de disco completo:** Para una capa adicional de seguridad para los datos en reposo, recomendamos usar herramientas de cifrado de disco completo como **Microsoft BitLocker**. BitLocker soporta cifrado AES (128 y 256 bits) y puede proteger todo el volumen del sistema operativo, volúmenes de datos o unidades virtuales.

3.3 Almacenamiento y transmisión segura de contraseñas

- **Contraseñas de G-Core:** Las contraseñas en G-Core se hashean usando el **Algoritmo de Hash Seguro (SHA−256).** La transmisión de contraseñas se cifra dualmente: primero usando **Blowfish** (un cifrado por bloques de clave simétrica) y segundo, usando cifrado estándar de contraseñas de Windows con salt(dato aleatorio que se genera en un proceso y que se guarda junto con el hash), que está vinculado a la máquina Windows específica.
- **Contraseñas G-SIM:** Las contraseñas G-SIM se almacenan utilizando el **algoritmo estándar de la industria PBKDF2 con salting** que proporciona una fuerte protección contra ataques de fuerza bruta.

4 Guía de Endurecimiento del Sistema

"Endurecer" se refiere al proceso de asegurar un sistema reduciendo su superficie de vulnerabilidad. Aunque los sistemas Geutebrück se entregan con medidas clave de seguridad, se debe realizar un endurecimiento adicional durante la puesta en servicio según los requisitos específicos del sitio.

4.1 Actualizaciones de firmware y software

Mantén siempre actualizado el firmware y el software de todos los componentes (cámaras, servidores, clientes, switches de red). Esto garantiza que el sistema esté protegido por los últimos parches de seguridad disponibles. Consulta regularmente el Portal Geutebrück para actualizaciones y las páginas web de los fabricantes para dispositivos de terceros.

4.2 Control físico de acceso

El acceso físico a servidores, estaciones de trabajo, cámaras y periféricos de red debe restringirse solo al personal autorizado. Esto evita manipulaciones, como la conexión no autorizada de dispositivos USB, la retirada de discos duros o la desconexión de cables.

4.3 Configuración y seguridad de la red

- **Segmentación de red:** La red de videovigilancia debe estar físicamente separada de la red corporativa principal del cliente. Si la separación física no es factible, se utilizan **VLANs** para segmentar lógicamente la red. Una práctica común es colocar las cámaras en una VLAN separada de los clientes de visualización.
- **Cortafuegos:** Utiliza un cortafuegos de última generación y probado en la industria para proteger el sistema de accesos no autorizados y para mitigar el riesgo de ataques de Denegación de Servicio (DoS) o Denegación de Servicio Distribuida (DDoS), especialmente si el sistema está conectado a otras redes o, a internet.
- **Seguridad de puertos y vinculación MAC:** En switches de red, activa funciones como **autenticación basada en puertos (IEEE 802.1X)** o **vinculación de direcciones MAC**. Esto garantiza que solo los dispositivos autorizados puedan conectarse a un puerto de switch, evitando accesos no autorizados a la red.
- **LAN inalámbrica (WLAN):** Evita usar LAN inalámbrica dentro de la red CCTV segura siempre que sea posible debido al aumento de los riesgos de seguridad.
- **Acceso remoto:** El acceso remoto a cualquier parte del sistema debe gestionarse mediante una **Red Privada Virtual (VPN) segura** utilizando estándares modernos de cifrado y autenticación. Nunca expongas un sistema directamente a internet sin protección contra cortafuegos. Si el reenvío de puertos es absolutamente necesario, solo reenvía los puertos mínimos requeridos y restringe el acceso a las direcciones IP de origen autorizadas.

4.4 Endurecimiento de dispositivos y aplicaciones

- **Desactivar los servicios no utilizados:** Desactivar todos los servicios no utilizados en cámaras y servidores de Windows para reducir la superficie de ataque. Esto incluye servicios como SSH, multicast o QoS en cámaras si no se requieren, y servicios como SNMP en Windows si no se utiliza ningún sistema de monitorización.
- **Cambiar puertos predeterminados:** Para dispositivos como cámaras, cambia los puertos de administración y streaming por defecto para que sean menos susceptibles a ataques automáticos.
- **Acceso a bases de datos SQL:** Para cualquier análisis o informe sobre la base de datos SQL, utilice una cuenta con los permisos mínimos necesarios para la lectura. No uses la cuenta de administrador de sistemas para consultas rutinarias.

4.5 Gestión de usuarios y acceso

- **Cambiar contraseñas predeterminadas:** Cambiar inmediatamente todas las contraseñas predeterminadas de administrador (sistema Geutebrück, cámaras, interruptores) por contraseñas fuertes y únicas que cumplan con estándares modernos de complejidad (por ejemplo, la política de contraseñas OWASP). Las contraseñas deben cambiarse regularmente.
- **Principio de Privilegio Mínimo:** Configurar los derechos de usuario para que los individuos solo tengan acceso a las funciones y datos necesarios para su función. El software de Geutebrück permite un control granular sobre los permisos de usuario.
- **Cuentas de servicio de Windows:** Los servicios Geutebrück se ejecutan por defecto como "LocalSystem". Si se utiliza una cuenta de servicio dedicada, asegúrate de que tenga una contraseña fuerte y solo derechos de usuario local. No se requiere una cuenta de administrador de dominio y se desaconseja encarecidamente. Para la sincronización LDAP en G-SIM, la cuenta de servicio solo requiere permisos de lectura en Active Directory.
- **Cierre automático de sesión:** Configura G-SIM para que cierre sesión automáticamente a los usuarios tras un periodo de inactividad especificado (por ejemplo, 15-60 minutos). Del mismo modo, configura Windows para bloquear automáticamente la sesión de pantalla tras un breve periodo de inactividad.
- **UAC en clientes:** La mayoría de las aplicaciones cliente Geutebrück no requieren derechos de administrador para ejecutarse. Esto ayuda a contener el posible impacto del malware en una estación de trabajo cliente.

5 Gestión de Seguridad Continua

La seguridad es un proceso continuo, no una configuración puntual.

5.1 Actualizaciones de seguridad y gestión de parches de Microsoft Windows

Instalar actualizaciones de seguridad de Microsoft es fundamental. Sin embargo, es esencial verificar primero que estas actualizaciones no afecten negativamente al rendimiento y la estabilidad del sistema Geutebrück. Geutebrück ofrece un servicio integral **de gestión de parches** para apoyar a los clientes, que incluye:

1. **Clasificación:** Comprobamos, clasificamos ("Crítico", "Importante", "No Relevante") y documentamos todas las nuevas actualizaciones de Microsoft, proporcionando recomendaciones sobre su aplicabilidad al software Geutebrück.
2. **Instalación:** Según la clasificación, nuestros expertos pueden realizar la instalación de parches aprobados, asegurando un despliegue controlado.
3. **Pruebas:** Tras la instalación, realizamos pruebas funcionales en el software Geutebrück para verificar que el funcionamiento del sistema se mantenga estable y eficiente.

5.2 Compatibilidad de software antivirus

Se recomienda utilizar un antivirus actualizado. Para garantizar que el rendimiento del sistema no se deteriore, es esencial configurar el software antivirus con las siguientes excepciones:

- Excluye la base de datos de vídeo Geutebrück de los escaneos en tiempo real y programados.
- Añadir carpetas y bibliotecas de aplicaciones Geutebrück a la lista blanca/lista de excepciones de escaneo de seguridad.

5.3 Gestión y soporte de vulnerabilidades

Geutebrück supervisa activamente el mercado en busca de amenazas emergentes y posibles vulnerabilidades.

- **Respuesta rápida:** Las vulnerabilidades detectadas o reportadas se analizan inmediatamente y las correcciones se priorizan según su criticidad.
- **Comunicación abierta:** Mantenemos una cultura de información abierta e informamos rápidamente a socios y clientes sobre las brechas de seguridad identificadas y las soluciones disponibles.
- **Soporte Central:** Nuestro equipo de Soporte Central está disponible para ofrecer asesoramiento experto y asistencia en la implementación de medidas para abordar vulnerabilidades de seguridad.