FEELS RIGHT.

Ergonomie, Bedienkonzept, System- und IT-Sicherheit

Die Herausforderung

- Komplexere Anwendungen
- größere Datenmengen
- mehr Monitore
- Virtualisierung als Vereinfachung und zugleich Herausforderung

Lösungswege:

- Arbeitsplatzergonomie
- Anwender im Fokus
- Prozesse begreifbar und übersichtlich machen
- Zur richtigen Zeit die richtigen Informationen (Systeme) in Zugriff bringen

Security first!

Sichere IT Infrastrukturen in der Leitstelle
und Anwenderorientierte Bedienkonzepte mit KVM

NIS2-Anforderungen und deren Auswirkungen auf die Leitstellensysteme

„Pflichten für Betreiber“

1. Awareness

→ steigt gerade, natürlich die Aufgabe das hochzuhalten („individuelles Assessment zu Maßnahmen“)

2. Physikalische Sicherheit & Personal

→ Rechner zugriffsgeschützt unterbringen

3. Prävention

→ Redundanz und Netztrennung

4. Krisen- & BCM (Business Continuity Management)

→ Geo-Redundanz, Systemzugriff „von außen“

Risikominimierung, Prävention und Business Continuity

→ KVM kann entscheidenden Beitrag leisten

Was bedeutet das für die Sicherheits-anforderungen an das KVM-System?

Informations-Sicherheits-Management-System
(Information Security Management System)

Verfahren und Regeln innerhalb einer Organisation, die dazu dienen, die Informationssicherheit dauerhaft zu definieren, zu steuern, zu kontrollieren, aufrechtzuerhalten und fortlaufend zu verbessern

Schützt uns als Unternehmen

- Intellectual Property
- Business Intelligence (Kundeninformationen)
- Business Continuity Management

→ Wesentlicher Schutz innerhalb der Lieferkette

Produktanforderungen

Sicherheitsmerkmale
– im Standard enthalten –

Für Zertifizierungen relevant, u.a. ‚NERC CIP' (North American Electric Reliability Corporation Critical Infrastructure Protection)

Trusted Platform Module (TPM)

- Bootloader, Betriebssystem und Firmware bilden eine vertrauenswürdige Plattform zum Schutz des Systems vor Manipulationen durch Dritte
- stellt sicher, dass ein Gerät nur mit Software gebootet wird, die vom Originalhersteller als vertrauenswürdig eingestuft wurde

Verschlüsselung

Proprietäres Protokoll für dedizierte Verbindungen bei KVM-over-IP ergänzt um volldynamische Verschlüsselung.

→ Methoden für ständige Schlüsselmodifikation und Vorwärtssicherheit:

- Sehr sicherheitsrelevante K/M sowie Steuerdaten und VPN verwenden AES256 Galois/Counter Mode (GCM), Schlüsselwechsel zufällig im Bereich 40 bis 80 Minuten
- Hochgeschwindigkeitsdaten (Video, Audio, GenUSB) verwenden AES128 Counter Mode (CTR), Schlüsselwechsel zufällig im Bereich 3 bis 5 Stunden oder bei Umschaltereignissen

Passwortkomplexität

- Systemweite Vorgabe von minimaler Passwortlänge,
  Mindestanzahl Groß-/Kleinbuchstaben,
  Mindestanzahl Ziffern,
  Mindestanzahl Sonderzeichen,
  Mindestanzahl der zu verändernden Zeichen des vorherigen Passworts

Anmeldeoptionen

- Anzahl gleichzeitiger Sitzungen mit Superuser-Recht beschränkbar (nur bei KVM-over-IP Matrix Systemkomponenten)
- Anzahl aufeinanderfolgenden ungültigen Anmeldeversuche bis Sperrzeitpunkt definierbar
- Anzeige von Nutzungsmeldungen vor Gewährung des Gerätezugriffs konfigurierbar

UID-Locking

- Beschränkung der Kommunikation auf vertrauenswürdige Geräte

Logging und Monitoring

- Darstellung von Systemzuständen
- Meldung von Anmeldevorgängen, Konfigurationsänderungen

Update und Backup/Restore

- Sichere, geschützte Updates
- Auto-Backup-Funktion für regelmäßiges Systembackup

Produktanforderungen

Sicherheitsmerkmale
– Zusatzoptionen –

2-Faktor-Authentifizierung (2FA)

- Erhöhte Sicherheit durch Verwendung reguläres Benutzerpasswort kombiniert mit zeitbasiertem Einmalpasswort (TOTP).
- Sowohl Software-Token als auch Hardware-Token unterstützt.
- Bei zweistufiger Challenge-Response-Authentifizierung werden Benutzerkennwort und zeitbasiertes Einmalkennwort nacheinander eingegeben, verschiedene Konfigurationsmöglichkeiten:
- Verwendung interner G&D-Authentifizierungsserver
- Verwendung externer Authentifizierungsserver
- Benutzerverwaltung intern im G&D-Gerät oder über unterstützte Verzeichnisdienste (Active Directory o.ä.)

DirectRedundancyShield (DRS)

- Schützt KVM-Installation durch Implementierung eines redundanten KVM-over-IP-Matrixsystems, das bei Ausfall des vorherigen Systems sofort Betrieb übernimmt
- Sobald DRS-Funktion konfiguriert, stellen jedes Benutzer- und Computermodul zwei permanente Verbindungen zum aktiven u. passiven KVM-over-IP-Matrix-Switch über das Netzwerk her, wobei nur eine Übertragungsleitung verwendet wird.
- Wenn eine Verbindung unterbrochen wird, übernimmt die vorherige passive Verbindung automatisch und direkt.
- Das Umschalten erfolgt nahtlos und völlig ohne Verzögerung bei der Bildübertragung.

SecureCert

- Verwendung von zertifizierten Software-Komponenten und Einstellungen innerhalb der KVM-over-IP Matrixsystemkomponenten
- Verfügbar ab ca. Q4/2024 für ControlCenter-IP 2.0, ControlCenter-IP-XS, Vision-IP, VisionXS-IP, RemoteAccess-IP-CPU
- Betrifft die Zertifizierungen FIPS 140-3, DoDIN APL und CC EAL2+

Produktanforderungen

Sicherheitsmerkmale
– Zertifizierung für KVM-over-IP Produkte –

FIPS Pub 140-3

(Federal Information Processing Standard Publication 140-3)

- 140-3 beschreibt Sicherheitsanforderungen für kryptographische Module
- basiert auf den Normen ISO/IEC 19790:2012 und ISO/IEC 24759:2017
- gewährleistet einheitlichen Sicherheitsrahmen für in IT-Systemen verwendete Kryptografie
- Verantwortlich ist National Institute of Standards and Technology (NIST)
- Hauptsächlich relevant für USA & Kanada, besonders Behörden
- Level 1-Validierung über kryptografische Software-Komponente
- Grundlage für weitere Zertifizierungen
- Zertifizierung des G&D KVM-over-IP Matrixsystems
- Erhältlich via kostenpflichtigem Feature-Key ‚SecureCert' pro Gerät

FIPS 140-3™

DoDIN-APL

(Department of Defense Information Network Approved Products List)

- Konsolidierte Liste von Produkten, die Zertifizierung für Cybersicherheit u. Interoperabilität durchlaufen haben
- Verantwortlich ist Defense Information Systems Agency (DISA)
- Gemeinhin als UC APL, JITC Testing, STIG Testing, DISA Tested, etc. bezeichnet
- Hauptsächlich relevant für US-Militär (DoD, z.B. Army, Navy, etc.) und Geheimdienste
- Zertifizierung des G&D KVM-over-IP Matrixsystems als 'Video Distribution System over IP'
- Erhältlich via kostenpflichtigem Feature-Key ‚SecureCert' pro Gerät

DoDIN APL
APPROVED PRODUCT

CC (Common Criteria for Information Technology Security Evaluation) EAL2+

- Bietet allgemeine Kriterien für Bewertung der Sicherheit von Informationstechnologie
- internationaler Standard zur Prüfung und Bewertung der Sicherheitseigenschaften von IT-Produkten nach Norm ISO/IEC 15408:2022
- International gegenseitig bei 31 Ländern anerkannt nach CCRA bis EAL2 und nach SOGIS-MRA bis EAL 4
- Verschiedene internationale Modelle, die sich in den Anforderungen unterscheiden

Common Criteria

CC (Common Criteria for Information Technology Security Evaluation) EAL2+

- Bewertungsstufen für Umfang, Tiefe und Methoden der Prüfung werden im Allgemeinen gemäß EAL 1-7 (Evaluation Assurance Level, internationaler Gebrauch) und NIAP PP (Protection Profiles, US Gebrauch) beschrieben
- Ermöglicht es Anbietern, die Sicherheitsfunktionen des Produkts zu beschreiben und die Behauptungen zu belegen

CC EAL	Bedeutung
EAL1	funktionell getestet
EAL2	strukturell getestet
EAL3	methodisch getestet und überprüft
EAL4	methodisch entwickelt, getestet und durchgesehen

Common Criteria

CC (Common Criteria for Information Technology Security Evaluation) EAL2+

- G&D hat sich für die Umsetzung des weltweit anerkannten EAL2+ Standards entschieden, eng wie möglich an den von NIAP bekannten Schutzprofile und Spezifikationen
- EAL-Stufen erhöhen nicht die Sicherheit. Sie erhöhen nur die Zuverlässigkeit der Sicherheitsaussagen. Mit anderen Worten, sie erhöhen den Umfang der Nachweise, Tests und Überprüfungen, die anhand der Sicherheitsaussagen durchgeführt werden.

Common Criteria

CC (Common Criteria for Information Technology Security Evaluation) EAL2+

- Hauptsächlich relevant für US-Militär und -Geheimdienste, NATO sowie internationale militärischen Einrichtungen, steigender Bedarf erkennbar
- Zertifizierung des G&D KVM-over-IP Matrixsystems
- Erhältlich via kostenpflichtigem Feature-Key ‚SecureCert' pro Gerät

Sichere IT Infrastrukturen

- KVM-System als wesentliches Sicherheitsmerkmal
- Dadurch selbst kritische Komponente
- Resilienz durch Redundanz- und Sicherheitskonzepte
- Dokumentiert über internationale Zertifizierungsstandards, weitere Relevanz für KRITIS
- Kritische Betrachtung innerhalb des Unternehmens als Teil der Lieferkette

ISO/IEC 27001

FIPS 140-3™

DoDIN APL
APPROVED PRODUCT

Common Criteria