Zugriffsrechte für Leitstellen

Aufgabe: Eine Leitstelle soll für einen Kunden im Rahmen eines Sicherheitskonzeptes Bewachungsaufgaben wahrnehmen. Welche Rechte müssen am Videosystem die die Leitstelle freigegeben werden?

Systemumgebung

- Leitstellen, die EBÜS verwenden, u.a. → www.videoleitstellen.de
- Video-Sicherheit-Systeme (VSS), die in EBÜS integriert wurden → www.ebues.de/partner

Hintergrund

Leitstellen übernehmen Bewachungsaufgaben für ihre Kunden, die typischerweise die Eigentümer der zu bewachenden Objekte („Schutzobjekte“) sind. Grundlage dafür sollte ein fundiertes Sicherheitskonzept sein, in dem Aufgaben und Verantwortlichkeit der Leitstelle klar geregelt sind.

Lösung

Der Zugriff der Leitstelle auf die Videosysteme sollte über passende Accounts präzise auf den zur Erfüllung der Bewachungsaufgabe erforderlichen Funktionsumfang beschränkt werden. Keinesfalls dürfen Leitstellen Accounts mit Administrator-Rechten für die Videosysteme Ihrer Kunden erhalten.

Begründung

Aus Sicht eines Objektbetreibers ist es weder erforderlich noch sicherheitsgerecht, einer externen Leitstelle administrative Vollzugriffsrechte auf das eigene Videosicherheitssystem einzuräumen. Stattdessen ist es fachlich geboten, der Leitstelle ausschließlich einen rollenbasierten, streng begrenzten Zugriff zu gewähren, der sich exakt an den Anforderungen der Bewachungsaufgabe orientiert.

1. Grundsatz der minimalen Rechtevergabe (Least Privilege)

Der zentrale sicherheitstechnische Grund hierfür ist das anerkannte Prinzip der minimalen Rechtevergabe. Dieses besagt, dass jeder Benutzer – unabhängig davon, ob intern oder extern – nur genau die Berechtigungen erhalten darf, die zur Durchführung seiner konkreten Aufgabe zwingend erforderlich sind.

Für eine Leitstelle bedeutet dies:

- Zugriff nur auf die relevanten Kameras bzw. Kameragruppen
- Nutzung nur der für die Alarmbearbeitung notwendigen Funktionen
- Kein Zugriff auf Systemkonfiguration, Benutzerverwaltung oder sicherheitskritische Einstellungen

Ein darüber hinausgehender Zugriff widerspricht diesem grundlegenden Sicherheitsprinzip.

2. Reduzierung von Sicherheitsrisiken und Angriffsfläche

Jede zusätzlich vergebene Berechtigung erhöht die potenzielle Angriffsfläche eines Systems. Wird ein Konto mit erweiterten Rechten kompromittiert (z.B. durch Phishing, Fehlkonfiguration oder Insider-Bedrohung), kann der Schaden erheblich sein.

Durch die Beschränkung der Rechte:

- wird die Angriffsfläche reduziert
- wird das mögliche Schadensausmaß bei einem Sicherheitsvorfall begrenzt
- wird die Gefahr reduziert, dass sich Angreifer lateral im System ausbreiten

Admin-Rechte für eine Leitstelle würden hingegen bedeuten:

- vollständiger Zugriff auf alle Kameras und Daten
- Manipulationsmöglichkeiten an Konfiguration, Aufzeichnungen und Alarmregeln
- potenzielle Beeinträchtigung der gesamten Sicherheitsinfrastruktur

Das ist aus Risikoperspektive nicht vertretbar.

3. Schutz vor Fehlbedienung und unbeabsichtigten Systemeingriffen

Neben gezielten Angriffen stellen auch Bedienfehler ein relevantes Risiko dar.

Je höher die Rechte eines Benutzers:

- desto größer ist das Risiko unbeabsichtigter Änderungen
- desto schwerwiegender sind potenzielle Auswirkungen (z.B. Deaktivierung von Aufzeichnungen, Löschen von Daten, Fehlkonfiguration von Alarmen)

Ziel einer klar begrenzte Rollenvergabe ist, dass:

- die Leitstelle ausschließlich innerhalb ihres Aufgabenbereichs agieren kann
- systemkritische Funktionen vor unbeabsichtigtem Zugriff geschützt bleiben

4. Trennung von Verantwortlichkeiten (Separation of Duties)

Ein weiterer etablierter Sicherheitsgrundsatz ist die Funktionstrennung:

- Der Objektbetreiber bleibt verantwortlich für Systembetrieb, Konfiguration und Datensicherheit
- Die Leitstelle ist verantwortlich für die operative Überwachung und Alarmbearbeitung

Diese klare Trennung:

- reduziert Interessenkonflikte
- erschwert unkontrollierte Änderungen am System
- erhöht Transparenz und Nachvollziehbarkeit

Admin-Rechte würden diese Trennung aufheben und zu einer unklaren Verantwortungsstruktur führen.

5. Datenschutz und rechtliche Anforderungen (DSGVO)

Videoüberwachung greift in Persönlichkeitsrechte ein und unterliegt strengen datenschutzrechtlichen Anforderungen.

Daraus ergeben sich konkrete Pflichten:

- Zugriff auf personenbezogene Daten nur im erforderlichen Umfang
- Zweckbindung der Verarbeitung (nur zur Gefahrenabwehr / Alarmverifikation)
- Minimierung der Datenverarbeitung

Ein uneingeschränkter Admin-Zugriff der Leitstelle wäre hier problematisch, da:

- mehr Daten zugänglich wären als für die Aufgabe notwendig
- keine klare Zweckbindung mehr sichergestellt ist

Ein eingeschränkter Account unterstützt dagegen unmittelbar die Anforderungen aus:

- Art.32 DSGVO (Datensicherheit)
- Need-to-know-Prinzip

6. Nachvollziehbarkeit, Auditierbarkeit und Compliance

Eine saubere Rollen- und Rechtevergabe ist Voraussetzung für:

- klare Protokollierung von Zugriffen
- eindeutige Zuordnung von Aktionen zu Verantwortlichkeiten
- erfolgreiche Audits und Zertifizierungen (z.B. ISO27001)

Moderne Zugriffskonzepte fordern explizit:

- rollenbasierte Zugriffskontrolle (RBAC)
- regelmäßige Überprüfung von Berechtigungen
- Dokumentation aller Zugriffe

Ein Admin-Zugang für externe Partner erschwert diese Kontrolle erheblich.

7. Vertrauensschutz und Betreiberhoheit

Nicht zuletzt spielt auch die organisatorische Perspektive eine Rolle:

Der Objektbetreiber:

- ist Eigentümer und Verantwortlicher des Systems
- trägt das Risiko bei Ausfällen oder rechtlichen Problemen
- muss jederzeit die Kontrolle über System und Daten behalten

Ein eingeschränkter Leitstellenzugang stellt sicher, dass:

- die Hoheit über das System beim Betreiber verbleibt
- externe Dienstleister nur im definierten Rahmen tätig werden

Fazit

Die Vergabe von Administratorrechten an eine Leitstelle ist aus sicherheitstechnischer, organisatorischer und rechtlicher Sicht nicht erforderlich und nicht empfehlenswert.

Stattdessen ist es Best Practice, der Leitstelle einen rollenbasierten, strikt eingeschränkten Zugriff bereitzustellen, der:

- exakt auf die Bewachungsaufgabe zugeschnitten ist
- die Angriffsfläche minimiert
- Fehlbedienung verhindert
- Datenschutzanforderungen erfüllt
- Verantwortlichkeiten klar trennt

Damit wird ein optimaler Kompromiss zwischen operativer Effizienz der Leitstelle und maximaler Sicherheit sowie Kontrolle für den Objektbetreiber erreicht.

Konkrete Beispiele

Die Leitstelle hat üblicherweise die Aufgabe, das Kundenobjekt zu bewachen.

Die Leitstelle hat nicht die Aufgabe, das Videosicherheitssystemen (VSS) des Kunden zu konfigurieren und zu warten - das ist üblicherweise Aufgabe des Errichters.

Das bedeutet konkret:

Die Leitstelle soll
- zu bestimmten Zeiten (Virtueller Wächterrundgang) oder
- bei bestimmten Ereignissen (Alarmen)
- die Bilder ausgewählter Kameras ansehen und bewerten ("Alarmverifikation")

und - falls nötig - die mit dem Kunden vereinbarten Maßnahmen durchführen, beispielsweise
- Kameras nachführen (PTZ-Steuerung)
- Täteransprache per Audio
- Fernwirken (Licht, Türen, Schranken, Sirene, Nebel, ...)
- Interventionskräfte entsenden

Die Leitstelle soll üblicherweise am Videosystem des Kunden nichts verstellen und darf auch nur auf ausgewählte Kameras zugreifen

Der Kunde hat möglicherweise auch private Kameras, die von der Leitstelle nicht gesehen werden sollen

Der Kunde hat auf seinem Videosystem Aufzeichnungen und Alarmregeln konfiguriert, die von der Leitstelle nicht geändert werden sollen

Errichter haben andere Aufgaben als die Leitstellen und benötigen deshalb eigene Accounts mit Rechten die ihrer Rolle angemessen sind.

Mitunter sind Sicherheitsunternehmen sowohl als Leitstelle als auch als Errichter tätig. Aber auch dann werden diese Aufgaben von unterschiedlichen Personen wahrgenommen und sollten durch jeweils passende Accounts abgesichert werden.

Gültigkeitsbereich: Dieser Hinweis gilt für EBÜS ab Version 2.2.1

Quellen / weiterführende Informationen

[1] → https://www.lfd.niedersachsen.de/faq/videouberwachung/faq-videouberwachung-175245.html
[2] → https://www.preeco.de/de/glossar/informationssicherheit/least-privilege
[3] → https://owasp.org/www-community/controls/Least_Privilege_Principle
[4] → https://netwrix.com/de/cybersecurity-glossary/architectural-concepts/least-privilege/

Stand: 19.06.2026, Dipl.-Ing. Hardo Naumann