

SICHER WISSEN, WAS SIE TUN

Mit dem **OC|Protokollserver** schaffen Sie eine zentrale Lösung für alle Systeme gemäß BSI IT-Grundschutz, ISO/IEC 27001 und EU-DSGVO Kompendium

Schnell ist es passiert, ein Sicherheitsvorfall sorgt für negative Schlagzeilen und die IT steht im Fokus. Oder das Parlament stellt eine Anfrage und Ihre Behörde ist in der Nachweispflicht. Wie nun belegen, dass kein strukturelles Problem vorliegt, sondern dass jemand einen individuellen Fehler gemacht hat? Oder gar Kriminelle Schuld an der Lage sind. Studien von Kaspersky belegen, dass die größte Gefahr von innen kommt, also von Beschäftigten in der eigenen Organisation. Aber wie kommen Sie Leuten auf die Spur, die willentlich oder unwillentlich dafür gesorgt haben, dass interne Daten das Haus verlassen konnten?

Mit unserem **OC|Protokollserver** protokollieren Sie die Zugriffe auf sämtliche Systeme und speichern diese integritätsgeschützt ab. Auf diese Weise werden Leaks nachverfolgbar und die Wahrscheinlichkeit steigt, dass illegale Eingriffe auffallen, bevor sie Schaden anrichten. Der Server lernt Ihre Systeme an und warnt Sie, sobald er einen verdächtigen Zugriff entdeckt. Oder anders: Sie wissen nun sicher, was Sie tun. Den **OC|Protokollserver** setzen wir bereits in Behörden mit allerhöchsten Sicherheitsanforderungen ein. Er steht Ihnen out-of-the-box zur Verfügung. Sprechen Sie uns an.

Protokolldaten schützen

IT-Sicherheitsabteilungen müssen den Zugriff auf schützenswerte Daten und Systeme jederzeit belegen können. Ein verantwortungsvoller Umgang mit personenbezogenen Daten ist dabei kein Nice-to-have. Er ist gesetzlich verpflichtend und fester Bestandteil des Risk- und Business Continuity Managements. Der OC|Protokollserver erlaubt dies.

IT-Systeme werden zunehmend verteilter und komplex. Die Protokollierung wird hier häufig von jeder Anwendung individuell abgedeckt, einfach nur ins Dateisystem geschrieben oder im Zweifel auch gar nicht abgebildet. Für die Sicherheitsbeauftragten eine Katastrophe: Wenn es darum geht, Leaks zu verfolgen und Zugriffe nachzuweisen, tappen sie im Dunkeln.

Dabei ist zu beachten, dass Protokolldaten mindestens so sensibel sind wie die Daten der Anwendungssysteme, die sie schützen möchten. Sie enthalten oft personenbezogene Daten von Mitarbeitenden oder der Kundschaft. Diese müssen bei einem Sicherheitsverstoß zur Verfügung stehen, dürfen aber nur in definierten Situationen und durch besonders berechnete Personen ausgewertet werden.

Wer behält den Überblick?

Erfolgt die Protokollierung in jeder einzelnen IT-Applikation, muss bei jedem System sichergestellt werden, dass die Protokollierung lückenlos erfolgt und die Daten integer sind. Für heterogene Anwendungslandschaften, die im Zuge der Digitalisierung weiterwachsen, hat das Konsequenzen:

- Die Anzahl der Protokolldaten steigt.
- Auswertungsmöglichkeiten fehlen.
- Der Aufwand für die Administration wird größer.
- Das Monitoring muss höhere Anforderungen erfüllen.
- Gesetzliche Löschfristen werden nicht eingehalten.

Warum eine zentrale Lösung?

Ein zentraler Protokollserver ermöglicht es Ihnen, die Übersicht zu behalten und Protokolldaten einheitlich auszugeben. Sie definieren die Sicherheitsanforderungen an einer Stelle und rollen sie von hier für die gesamte Organisation aus. Unterschiedliche Ausgabeformate, Matching-Probleme und Überwachungslücken gehören der Vergangenheit an.

Was macht der OC|Protokollserver genau?

Über verschiedene Schnittstellenmodule sammelt der **OC|Protokollserver** die Protokolldaten verschlüsselt über standardisierte Kommunikationsprotokolle ein und transformiert sie in ein einheitliches Protokollformat. Anschließend werden der Originaldatensatz und der Protokolldatensatz integritätsgeschützt im Archiv gespeichert. Die Daten werden hierbei mit einem asymmetrischen Verschlüsselungsalgorithmus signiert und auf Manipulationen hin überwacht.

Zusätzlich erfolgt die Speicherung in einem auswertbaren Index. Um Hardware- und Auswertungssysteme bei diesen riesigen Datenmengen handhabbar zu machen, verfügt der Protokollserver über unterschiedliche Strategien. Mittels Teil-Indizierung einzelner Anwendungssysteme kann er neue Daten ad hoc auswerten oder gezielte Auswertungen auf historische Daten vornehmen. Die Zugriffe werden dabei über ein Rollen- und Rechtekonzept eingeschränkt und die abgefragten Daten wiederum protokolliert (Selbstprotokollierung).

Vorteile für die ganze Organisation

Beschleunigen Sie die Einführung neuer IT-Systeme, indem Sie mit dem **OC|Protokollserver** einheitliche Sicherheitsvorgaben für alle IT-Systeme schaffen.

- Der OC|Protokollserver überträgt Ihre Sicherheitsrichtlinien auf jede vorhandene und neue IT-Lösung.
- Durch den zentralen Zugriff können Sicherheitsvorfälle ressourcensparend analysiert werden.
- Die Protokollierung wird an zentraler Stelle konfiguriert. Damit können Löschrufen einheitlich erfüllt und Löschungen bei Bedarf temporär ausgesetzt werden.
- Ausfälle und Fehler des Protokollservers oder einzelner Schnittstellen erkennen Sie im Monitoring und können Sie früh beheben.

Die Lösung eignet sich für Organisationen, Behörden und Unternehmen mit einem erhöhten Sicherheitsbedarf.

Unser Angebot

Getting Started!

In einem eintägigen Workshop

- ermitteln wir den Schutzbedarf Ihrer Protokolldaten,
- erörtern wir den Einsatz des OC|Protokollservers in Ihrer IT-Landschaft.
- Ziel ist ein individuelles Angebot für Ihre Organisation.

Unsere Leistungen

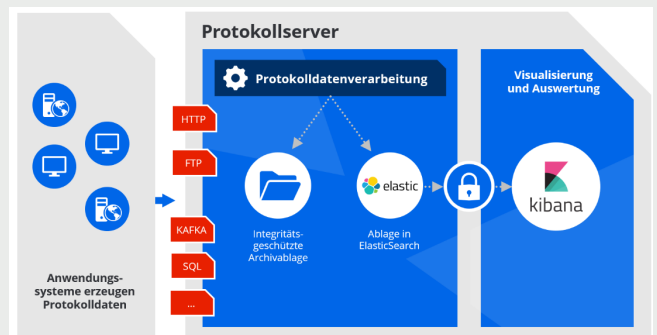
- Integration des Servers in Ihre IT-Landschaft
- Anbindung der Schnittstellen
- Abgleich mit bestehenden Sicherheitsvorgaben
- Kontinuierliche Weiterentwicklung und Betrieb

Ihre Vorteile

- Einfachere Erfüllung von Sicherheitsanforderungen
- Weniger Risiko und Aufwand
- Abkopplung des technischen Services
- Einfache Skalierbarkeit der Schnittstellen
- Erweiterung des Speicherplatzes
- Ausfallschutz durch Monitoring

Technologie & Aufbau

Welche Technologien und welche Architektur stecken im OC|Protokollserver?



Sprechen Sie uns an!



Andreas Fröhlich
Senior Manager Sales
+49 2261 6001-1064
andreas.froehlich@opitz-consulting.com

