Datenschutz und Betriebsrat bei CosyTrack.Drive



WISSEN

Alles zu CosyTrack.Drive: Laufwerksquellen, Arbeitsplatz und Terminalserver, Steuerung per GPO oder Intune an einem Ort.

› **CosyTrack.Drive**

BERATUNG

Du willst Protokoll, Leistungszähler und Vereinbarung vor dem Rollout sauber zusammenbringen? Wir gehen es mit dir durch.

› **Beratung zu CosyTrack.Drive**

SCHULUNG

Onboarding für die IT und Kurzschulung für die Belegschaft, inklusive der Frage, wer was sehen darf.

› **Schulung und Onboarding für CosyTrack.Drive**

Es gibt zwei Sorten von IT-Projekten: die, bei denen der Betriebsrat von Anfang an am Tisch sitzt, und die, bei denen er drei Tage vor dem Rollout davon erfährt. Die zweite Sorte erkennt man daran, dass der Go-live-Termin plötzlich „verschoben“ heißt und die Projektleitung anfängt, Sätze mit „eigentlich wollten wir doch nur“ zu beginnen. Wer SharePoint, Teams und OneDrive als Laufwerksbuchstaben einbindet, landet zuverlässig in dieser Diskussion. Denn ein Laufwerk, über das die ganze Belegschaft ihre Dateien öffnet und speichert, ist eine technische Einrichtung, die eine Menge darüber weiß, wer wann was getan hat.

Dieser Beitrag nimmt das Thema ernst, ohne es zu dramatisieren. Er zeigt zuerst, welche Spuren Microsoft 365 mit Bordmitteln ohnehin hinterlässt, denn die sind älter als jedes Zusatzprodukt und meist schon Gegenstand einer Vereinbarung. Danach geht es darum, was CosyTrack.Drive auf dem Arbeitsplatz oder Terminalserver protokolliert und misst, wofür, wie lange und wer es sehen kann. Und schließlich darum, was in eine Betriebs- oder Dienstvereinbarung gehört, damit das Protokoll bleibt, was es sein soll: ein Werkzeug für den Betrieb, kein Fernglas auf die Schreibtische.

FAKTEN · Kurz und bündig

CosyTrack.Drive bindet SharePoint- und Teams-Bibliotheken sowie OneDrive als Windows-Laufwerksbuchstaben ein, auf Windows-Arbeitsplätzen ebenso wie auf Terminalservern. Der Agent spricht ausschließlich mit Microsoft 365 im eigenen Tenant. Er sendet keine Telemetrie und hat keinen Kanal zum Hersteller, auch die Lizenz wird offline geprüft.

Das Aktivitätsprotokoll liegt pro Benutzer lokal, ist nur für den Benutzer, SYSTEM und Administratoren lesbar und wird standardmäßig nach 30 Tagen oder ab 200 MB bereinigt. Die Leistungszähler tragen Sitzungs- und Laufwerksnamen statt Personennamen und liegen nur im Speicher, bis jemand bewusst einen Datensammler anlegt.

KEIN RECHTSRAT · Was dieser Beitrag ist und was nicht

Hier schreibt eine IT-Beratung, keine Kanzlei. Der Beitrag beschreibt Technik und bewährte Organisation. Ob und wie weit in deinem Haus Mitbestimmungsrechte greifen, welche Rechtsgrundlage für eine Verarbeitung trägt und wie eine Vereinbarung formuliert sein muss, klärst du mit Datenschutzbeauftragten, Betriebs- oder Personalrat und im Zweifel mit Rechtsberatung.

Das Problem: Ein Laufwerk sieht alles, was über es läuft

Ein Fileserver hat nie gefragt, ob er protokollieren darf. Er hat es einfach nicht getan, zumindest nicht ohne Zutun, und wenn doch, dann in einem Sicherheitsprotokoll, das niemand gelesen hat, bis es voll war. Mit dem Umzug in die Cloud ändert sich das grundlegend. Moderne Dienste protokollieren, weil Sicherheit, Fehlersuche und Nachvollziehbarkeit ohne Protokoll nicht funktionieren. Das ist gut für den Betrieb und für die Sicherheit. Es heißt aber auch: Die Daten sind da, und Daten, die da sind, wecken Begehrlichkeiten.

Warum gerade Dateizugriffe heikel sind

Dateizugriffe sind besonders aussagekräftig. Aus „wer hat wann welche Datei geöffnet, gespeichert, umbenannt oder gelöscht“ lassen sich mit etwas bösem Willen Arbeitszeiten, Arbeitstempo und Arbeitsgewohnheiten ablesen. Niemand plant das beim Projektstart. Aber irgendwann fragt irgendwer, ob man „das nicht mal eben auswerten“ könne. Genau für diesen Moment braucht es Regeln, die vorher geschrieben wurden, nicht hinterher.

Mitbestimmung bei technischen Einrichtungen, ganz allgemein

In Betrieben mit Betriebsrat hat dieser nach dem Betriebsverfassungsgesetz ein Mitbestimmungsrecht bei der Einführung und Anwendung technischer Einrichtungen, die dazu geeignet sind, Verhalten oder Leistung der Arbeitnehmer zu überwachen. Im öffentlichen Dienst übernehmen die Personalvertretungsgesetze von Bund und Ländern diese Rolle, in kirchlichen Einrichtungen eigene Regelwerke. Der entscheidende Punkt für die Praxis: Es kommt in der Regel auf die Eignung an, nicht auf die Absicht. Dass du gar nicht überwachen willst, ist ein guter Vorsatz, ersetzt aber keine Beteiligung.

Daneben steht der Datenschutz. Protokolle mit Benutzerkonto, Rechnername und Dateipfad sind personenbezogene Daten. Damit gelten die bekannten Grundsätze: ein festgelegter Zweck, nicht mehr Daten als nötig, eine Löschfrist und klare Zugriffsrechte. Eine Betriebs- oder Dienstvereinbarung ist der Ort, an dem beides zusammenkommt, und sie ist erfahrungsgemäß der Weg, auf dem ein Rollout am wenigsten Überraschungen erlebt.

WARNUNG · Die teuerste Abkürzung

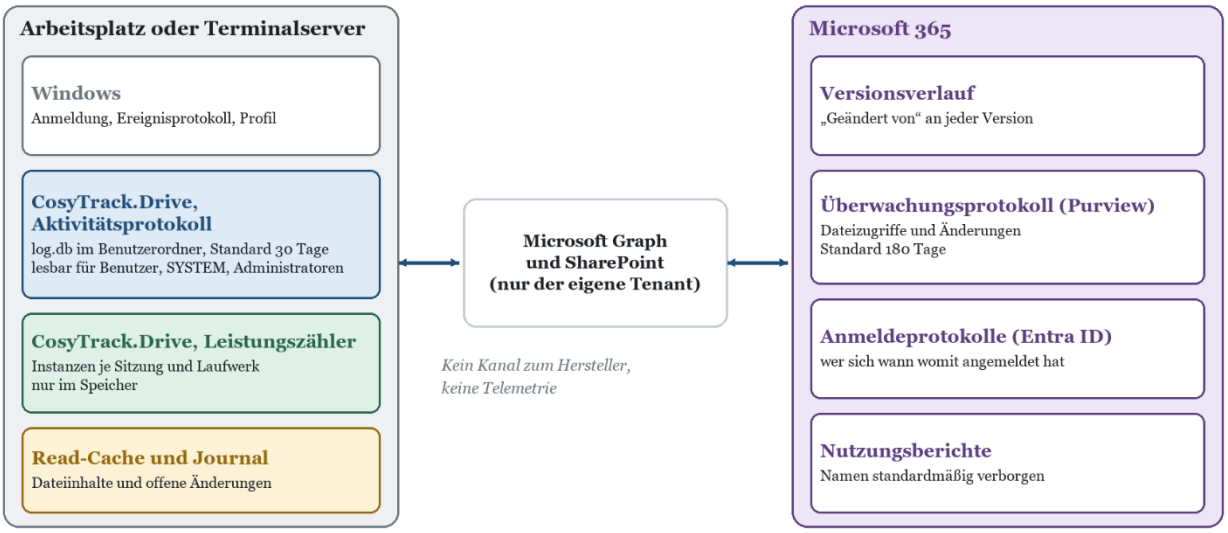
„Wir schalten erst mal ein und reden später mit dem Betriebsrat“ spart zwei Wochen und kostet im ungünstigen Fall das Projekt. Ein Gremium, das sich übergangen fühlt, prüft jedes weitere Vorhaben mit spitzerem Bleistift. Das gilt nicht nur für dieses Laufwerk, sondern für alles, was danach kommt.

Was Microsoft 365 mit Bordmitteln bereits protokolliert

Bevor über ein zusätzliches Protokoll gesprochen wird, lohnt der ehrliche Blick auf das, was schon da ist. Sobald Dateien in SharePoint, Teams oder OneDrive liegen, protokolliert Microsoft 365 eine ganze Menge, unabhängig davon, wie die Datei dorthin kam: per Browser, per Teams, per OneDrive-Synchronisierung oder per Laufwerksbuchstabe.

Wo beim Arbeiten mit Dateien Spuren entstehen

Ein Speichern, drei Orte: Windows, CosyTrack.Drive und Microsoft 365. Jeder führt sein eigenes Buch



Schematische Darstellung. Mitbestimmungsrelevant sind alle drei Orte, nicht nur der neue.

Quelle	Was festgehalten wird	Aufbewahrung	Wer es sieht
Versionsverlauf in SharePoint	jede Version mit Zeitpunkt und „Geändert von"	nach Versionseinstellungen der Bibliothek	alle mit Zugriff auf die Datei
Überwachungsprotokoll in Microsoft Purview	Dateizugriffe, Änderungen, Freigaben, Löschungen	Audit (Standard) 180 Tage, Audit (Premium) für SharePoint und OneDrive standardmäßig ein Jahr	Rollen mit Leserecht auf das Überwachungsprotokoll
Anmeldeprotokolle in Microsoft Entra ID	Anmeldungen mit Zeit, Anwendung und Ergebnis	ohne Entra ID P1/P2 sieben Tage, mit P1/P2 länger	Rollen mit Leserecht auf Protokolle
Nutzungsberichte im Microsoft 365 Admin Center	Aktivität pro Dienst	zeitlich begrenzte Berichtszeiträume	Administratoren, Namen seit September 2021 standardmäßig verborgen

Mit der Aufbewahrung im Überwachungsprotokoll lohnt ein genauer Blick, weil sie von Lizenz und Richtlinien abhängt und sich in den vergangenen Jahren geändert hat. Microsoft beschreibt die Details unter Aufbewahrungsrichtlinien für Überwachungsprotokolle (Microsoft Learn). Für die Vereinbarung heißt das: Diese Protokolle existieren bereits, und ihre Auswertung ist ebenso regelungsbedürftig wie die eines Zusatzprodukts.

FAKTEN · Gute Voreinstellung von Microsoft

Seit dem 1. September 2021 verbergen die Nutzungsberichte im Microsoft 365 Admin Center standardmäßig Benutzer-, Gruppen- und Websitenamen. Wer die Namen sichtbar machen will, muss die Organisationseinstellung bewusst ändern, und genau das wird im Überwachungsprotokoll vermerkt. Ein schönes Beispiel dafür, wie Technik Datenschutz unterstützen kann: nicht durch Verzicht auf Daten, sondern durch eine vernünftige Grundeinstellung und eine Spur, wenn jemand sie ändert.

Was die Bordmittel auf dem Rechner nicht sehen

Was Microsoft 365 nicht sieht, ist der Weg zwischen Anwendung und Cloud. Ob das Öffnen einer Datei in der Filiale zehn Sekunden dauerte, ob ein Upload wegen eines ungültigen Dateinamens hängt oder ob der Terminalserver gerade an seiner Plattengrenze kratzt, steht in keinem Überwachungsprotokoll. Genau hier setzen Protokoll und Leistungszähler von CosyTrack.Drive an. Sie erweitern die Datenlage also an einer Stelle, die für den Betrieb wichtig ist, und sie gehören deshalb in dieselbe Vereinbarung wie die Bordmittel.

TIPP · Gibt es schon eine Rahmenvereinbarung zu Microsoft 365?

Viele Häuser haben für Microsoft 365 eine Rahmenvereinbarung mit Anlagen pro Dienst oder Werkzeug. Dann ist CosyTrack.Drive keine neue Großbaustelle, sondern eine neue Anlage. Das spart Zeit und hält die Regeln an einem Ort zusammen. Fehlt eine solche Vereinbarung, ist das Laufwerksprojekt ein guter Anlass, sie anzugehen.

Was CosyTrack.Drive protokolliert, misst und speichert

Gute Gespräche mit Betriebsrat und Datenschutz beginnen mit einer ehrlichen Liste. Also: Was liegt wo, mit welchem Personenbezug, wie lange und wer kommt heran? Die folgenden Abschnitte beschreiben den Stand von Generation 60. Alle Stellschrauben sind Computerrichtlinien, die du per GPO oder Intune verteilst. Die Konfigurations-App zeigt dieselben Einstellungen zum Testen auf einem einzelnen Rechner. Einen Überblick über alle Funktionen und Laufwerksquellen findest du auf der Seite zu CosyTrack.Drive.

Kein Kanal zum Hersteller

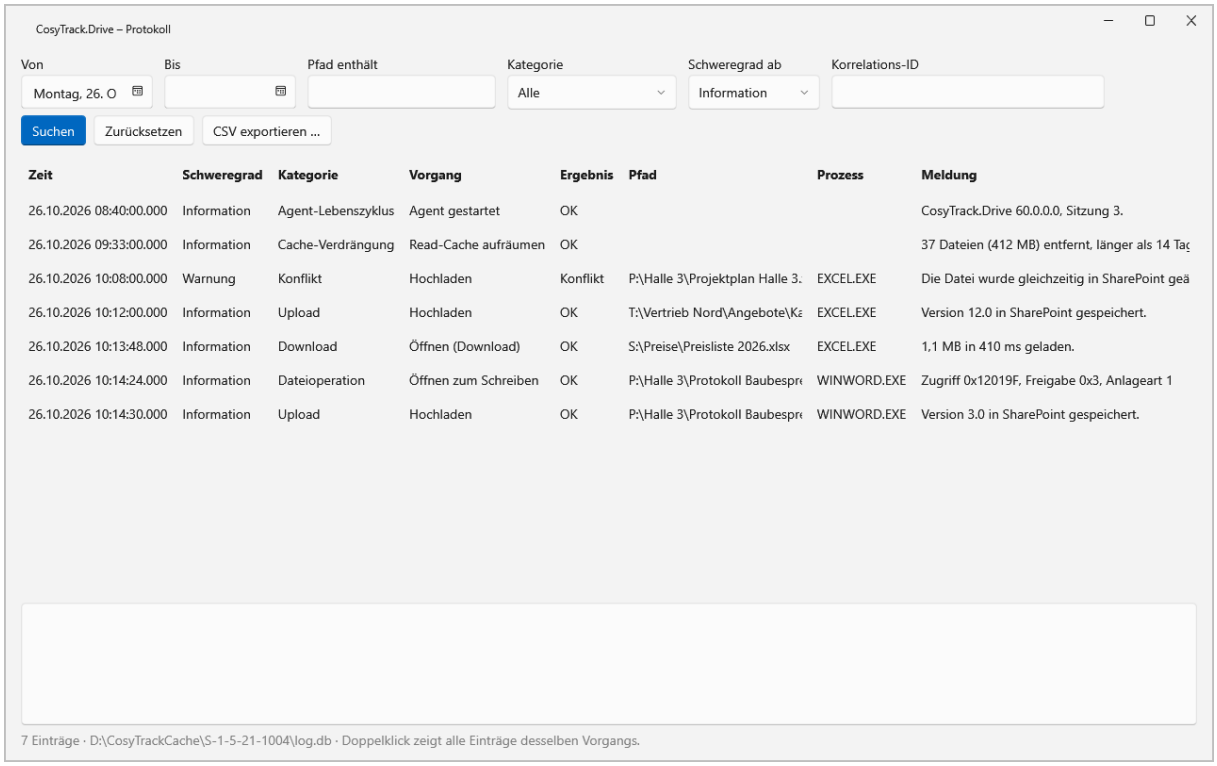
Die erste Frage im Gremium ist erfahrungsgemäß: „Und was schickt das Ding nach Hause?“ Die Antwort ist angenehm kurz: nichts. Der Agent spricht mit der Anmeldung bei Microsoft Entra ID, mit Microsoft Graph und mit SharePoint Online im eigenen Tenant. Es gibt keine Telemetrie an Dritte, keinen Update-Dienst, der im Hintergrund telefoniert, und keine Online-Lizenzprüfung. Die Lizenz wird offline anhand ihrer Signatur geprüft, der Testzeitraum nach der Installation läuft ebenfalls ohne Kontakt zum Hersteller.

Die Anwendung arbeitet in Microsoft Entra ID als öffentlicher Client ohne Client-Geheimnis und ausschließlich mit delegierten Berechtigungen. Sie handelt also immer im Namen des angemeldeten Benutzers und kann nur sehen, was dieser auch im Browser sehen dürfte. Eine Anwendungsberechtigung, mit der ein Dienst im Hintergrund quer durch alle Websites liest, gibt es nicht.

Das Aktivitätsprotokoll: nachvollziehbar, lokal, befristet

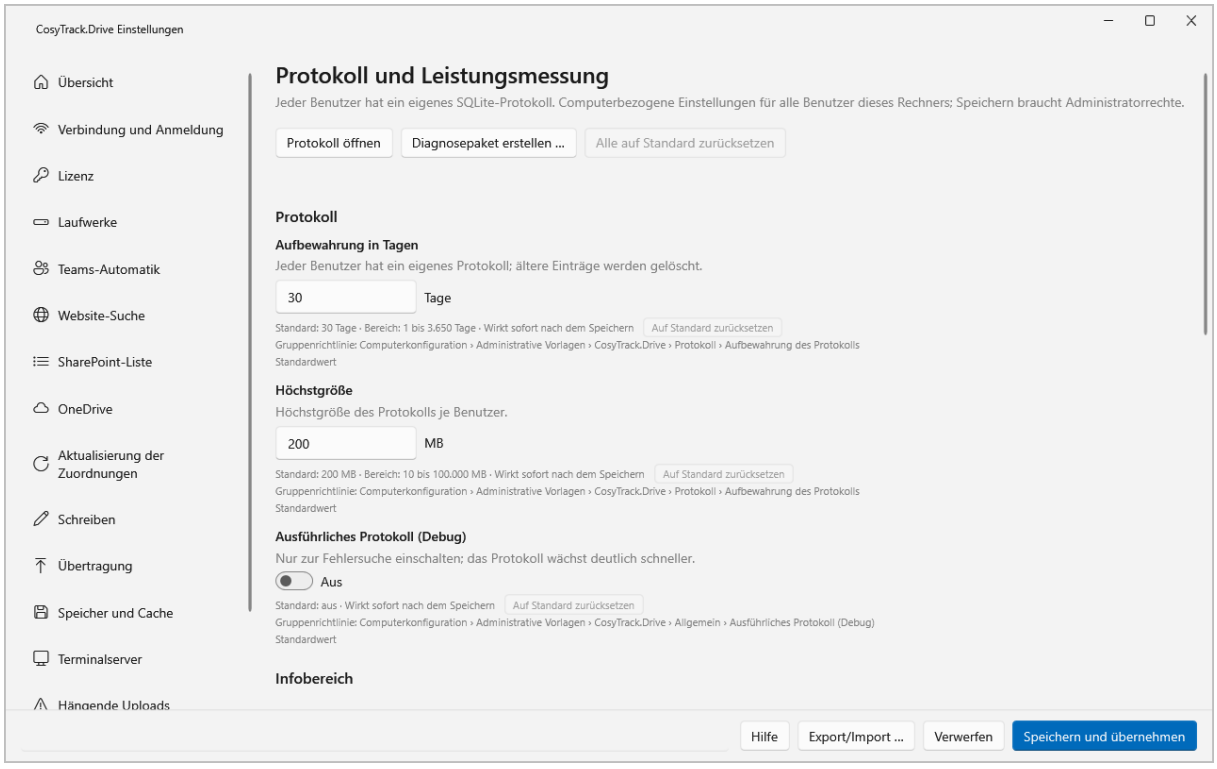
Das Aktivitätsprotokoll ist das Herzstück der Fehlersuche. Es hält Vorgänge wie Anmeldung, Download, Upload, Konflikt oder Aufräumen des Read-Caches fest, und zwar mit dem, was man zum Nachvollziehen braucht: Zeitpunkt, Kategorie, Ergebnis, Dateipfad, Prozess, Laufwerk, Ziel in SharePoint und Fehlertext. In jedem Eintrag stehen außerdem Windows-Konto, Anmeldename und Rechner. Das ist kein Versehen, sondern der Zweck: Wenn ein Benutzer fragt, warum seine Datei von Dienstag nicht in SharePoint angekommen ist, muss die IT genau diesen Vorgang finden können.

Wichtig für die Bewertung ist, wo das Protokoll liegt und wer herankommt. Die Protokolldatenbank liegt pro Benutzer im Cache-Verzeichnis auf dem jeweiligen Rechner oder Sitzungshost, nie auf einem Netzwerkpfad. Lesen dürfen sie der Benutzer selbst, SYSTEM und Administratoren des Rechners. Eine zentrale Sammelstelle, an die alle Agenten ihre Protokolle schicken, gibt es nicht.



Im Protokoll filterst du nach Zeit, Pfad, Kategorie oder Korrelations-ID, hier mit Demodaten von Erika Muster aus der Musterfirma GmbH.

Aufbewahrung und Größe stellst du mit der Richtlinie „Aufbewahrung des Protokolls“ ein. Standard sind 30 Tage und 200 MB pro Benutzer. Ältere Einträge und alles oberhalb der Höchstgröße löscht der Agent automatisch. Ob 30 Tage für euch passen, ist eine Frage für die Vereinbarung: Kürzer geht, wenn ihr Störungen schnell bearbeitet, länger kann sinnvoll sein, wenn Probleme erfahrungsgemäß erst nach Wochen auffallen. Das ausführliche Protokoll (Debug) ist standardmäßig aus. Es schreibt deutlich mehr Detail und gehört befristet in die Fehlersuche, nicht in den Dauerbetrieb.



Hier legst du Aufbewahrung und Höchstgröße des Protokolls fest und siehst, dass das ausführliche Protokoll standardmäßig aus ist.

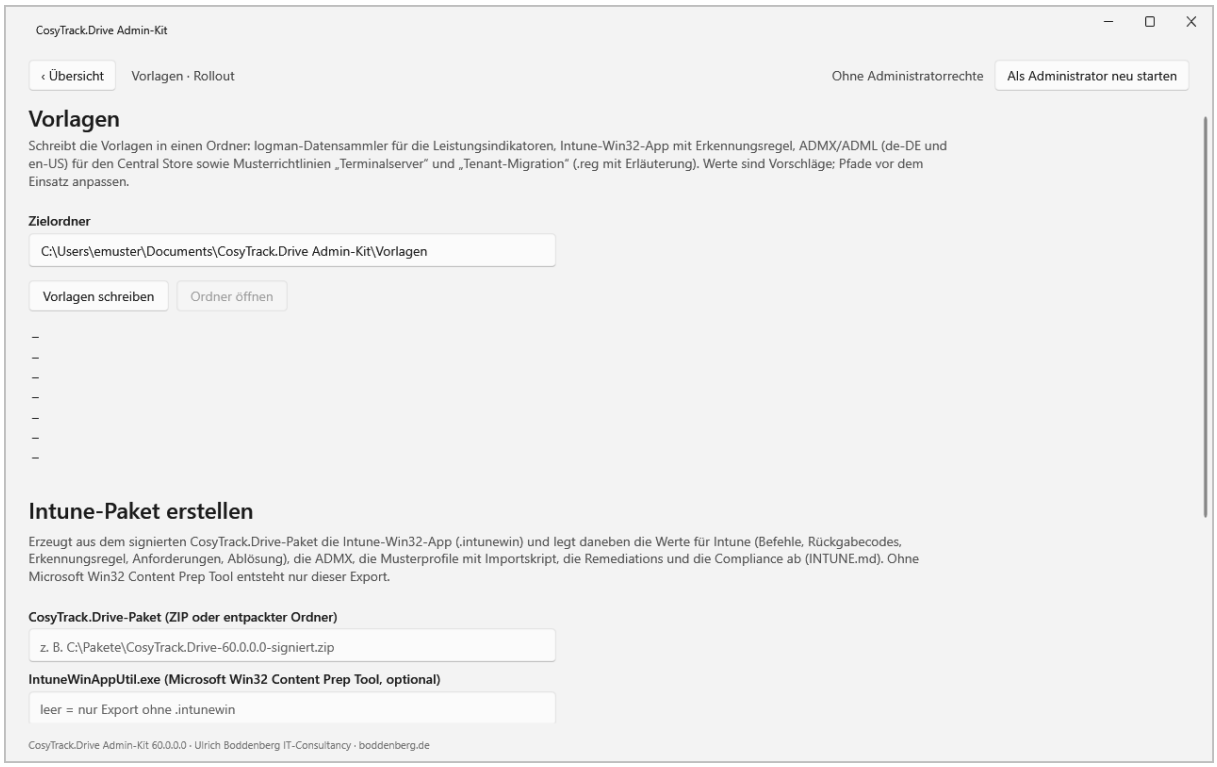
WICHTIG · Langsame Vorgänge ohne Dateinamen

Dauert ein Dateisystem-Aufruf länger als der eingestellte Schwellwert, schreibt der Agent einen Eintrag „Langsamer Vorgang“ mit Korrelations-ID, Vorgang, Dauer, Teilzeiten, Laufwerk und Größe. Dateinamen kommen dabei nur hinzu, wenn das ausführliche Protokoll per Richtlinie aktiv ist. Für die Frage „Wo geht die Zeit verloren?“ reicht das fast immer.

Leistungszähler: Sitzung statt Name

Die Leistungszähler sind der zweite Baustein. Jeder Agent veröffentlicht seine Messwerte als Windows-Leistungsindikatoren der Kategorie „CosyTrack.Drive“: von übertragenen Dateien über Wartezeit beim Öffnen und Drosselung durch Microsoft bis zur Übertragungsgeschwindigkeit. Die Instanzen heißen „_Total“ für den ganzen Rechner, „S3“ für eine Sitzung und „S3 S:“ für ein Laufwerk in dieser Sitzung. Personennamen kommen standardmäßig nicht vor. Die Werte liegen nur im Speicher. Das Statusfenster im Infobereich zeigt sie dem Benutzer für seine eigene Sitzung an, der Leistungsmonitor zeigt sie dem Administrator live.

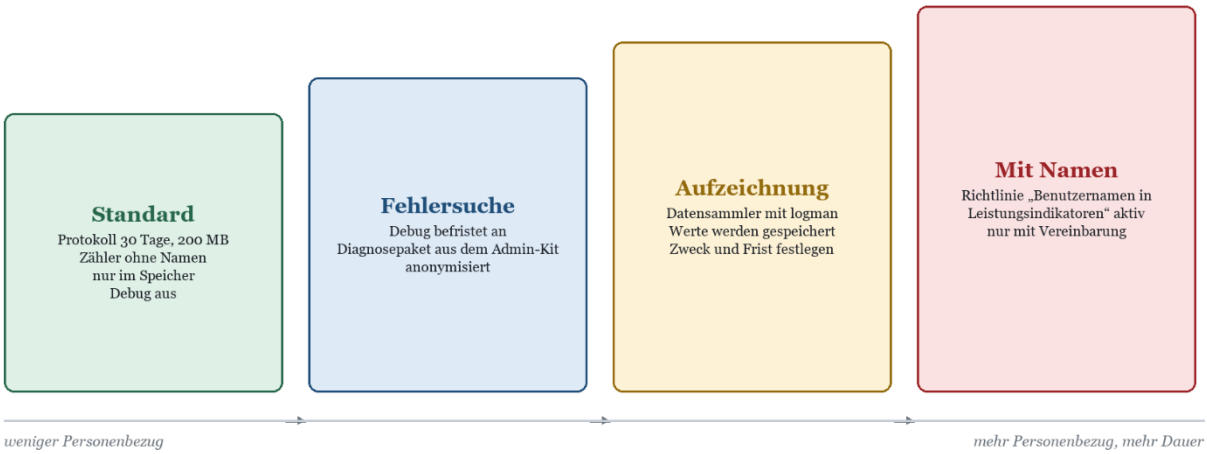
Zwei bewusste Schritte ändern das Bild. Erstens kann ein Administrator einen Datensammler anlegen, etwa mit logman oder einem Überwachungssystem, der die Werte dauerhaft speichert. Das Admin-Kit liefert dafür eine fertige Vorlage. Zweitens gibt es die Richtlinie „Benutzernamen in Leistungsindikatoren“, standardmäßig aus. Ist sie aktiv, tragen die Instanzen Benutzernamen, und auf dem Terminalserver kann jeder, der die Zähler lesen darf, sie sehen. Die Produktdokumentation weist an beiden Stellen ausdrücklich auf die Mitbestimmung hin, und die Konfigurations-App tut das ebenfalls. Wie du die Zähler sinnvoll für Standortvergleiche nutzt, beschreibt Microsoft-365-Anbindung messen mit Leistungszählern.



Unter „Vorlagen“ schreibt das Admin-Kit unter anderem den logman-Datensammler, den du bewusst und befristet einsetzt.

Die Regler, die du in der Hand hast

Jede Stufe nach rechts bedeutet mehr Personenbezug oder mehr Dauer. Und mehr Abstimmungsbedarf



Schematische Darstellung. Protokoll, Debug und Namen sind Richtlinien, Datensammler und Diagnosepaket bewusste Handgriffe.

TIPP · Zähler sind Thermometer, keine Stechuhr

Ein Thermometer im Serverraum sagt dir, dass es zu warm ist, nicht, wer die Tür offen gelassen hat. Genauso solltest du die Leistungszähler verwenden: pro Standort, pro Host, pro Laufwerk. Wenn eine Auswertung erst mit Namen interessant wird, ist sie in aller Regel keine Betriebsfrage mehr.

Ereignisprotokoll und Diagnosepaket

Was CosyTrack.Drive ins Windows-Ereignisprotokoll schreibt, wird vorher bereinigt: Adressen, Pfade, E-Mail-Adressen, Domänenkonten und Dateinamen werden ersetzt, Kennungen wie Drive-ID oder Tenant-ID erscheinen nur gehasht. Damit lassen sich Ereignisse gefahrlos in eine zentrale Überwachung übernehmen. Die bewusste Ausnahme sind Administratorhandlungen mit Folgen, etwa der Not-Aus für hängende Uploads oder das endgültige Löschen aus der Quarantäne. Dort steht die Kennung des ausführenden Administrators samt Begründung, und das ist auch gut so: Wer eingreift, soll nachvollziehbar sein.

Für die Fehlersuche mit dem Support erzeugt das Admin-Kit ein anonymisiertes Diagnosepaket. Benutzer, Anmeldenamen, Rechner, Adressen, Drive-IDs und Pfade werden dabei je Paket mit einem eigenen Zufallswert ersetzt, Tokens und Geheimnisse entfernt. Erhalten bleiben Prozessname, Laufwerksbuchstabe und Zeitstempel, weil ohne sie keine Fehlersuche möglich ist. Das Paket entsteht als lokale Zip-Datei. Verschickt wird es nur, wenn du es selbst verschickst.

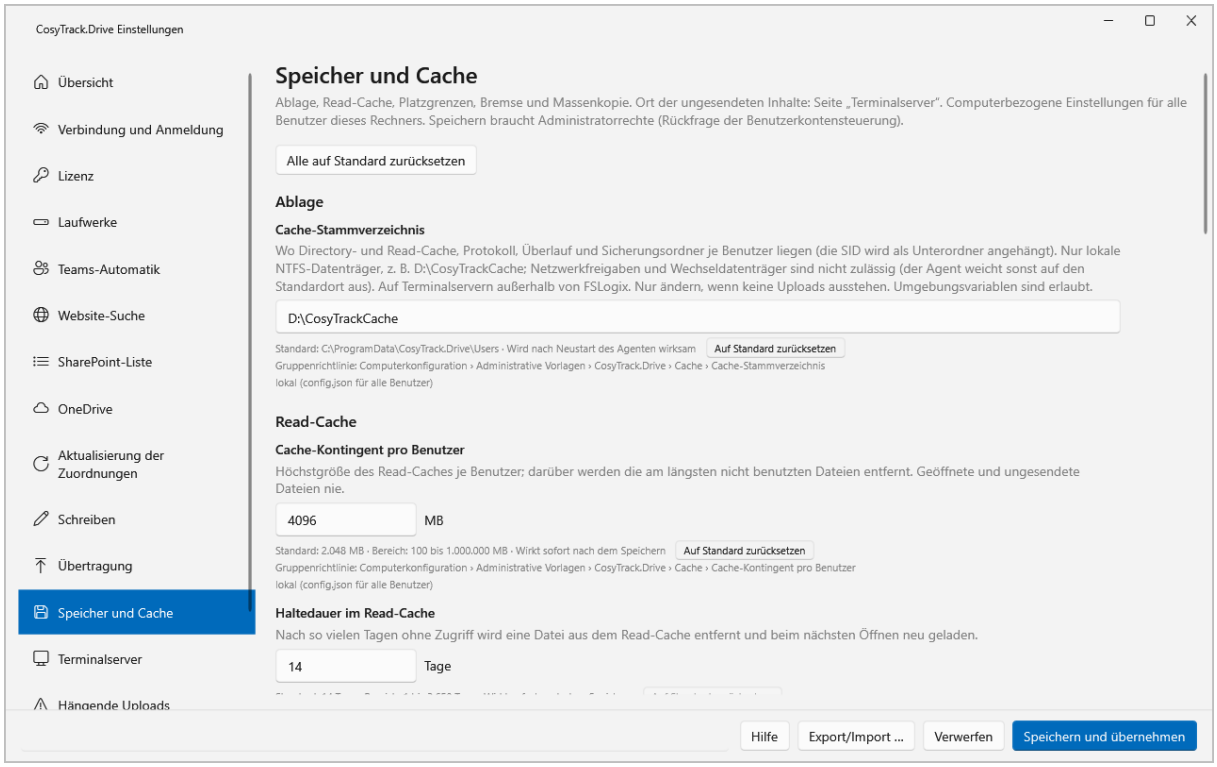
WARNUNG · Zwei Diagnosepakete, ein Unterschied

Auch die Konfigurations-App kann ein Diagnosepaket erstellen. Dieses entfernt Tokens und Geheimnisse, enthält aber Dateinamen, Pfade, Rechnernamen und Anmeldenamen im Klartext. Es ist für die Analyse im eigenen Haus gedacht. Für die Weitergabe an Dritte, also auch an deinen Dienstleister oder den Support, nimmst du das anonymisierte Paket aus dem Admin-Kit. Das gehört als Regel in die Vereinbarung.

Lokale Daten: Cache, Journal und ungesendete Inhalte

Damit ein Laufwerk schnell ist, hält CosyTrack.Drive Dateien im Read-Cache vor, und Änderungen warten im Journal und als ungesendete Inhalte, bis sie in SharePoint angekommen sind. Diese Daten sind durch Ordnerrechte geschützt, also nur für den Benutzer, SYSTEM und

Administratoren zugänglich, aber nicht eigens verschlüsselt. Wer Verschlüsselung im Ruhezustand verlangt, setzt BitLocker für die Volumes von Cache und Profil ein, was auf Notebooks ohnehin Standard sein sollte. Der Read-Cache wird nach einer einstellbaren Haltedauer ohne Zugriff und bei Erreichen des Kontingents aufgeräumt.

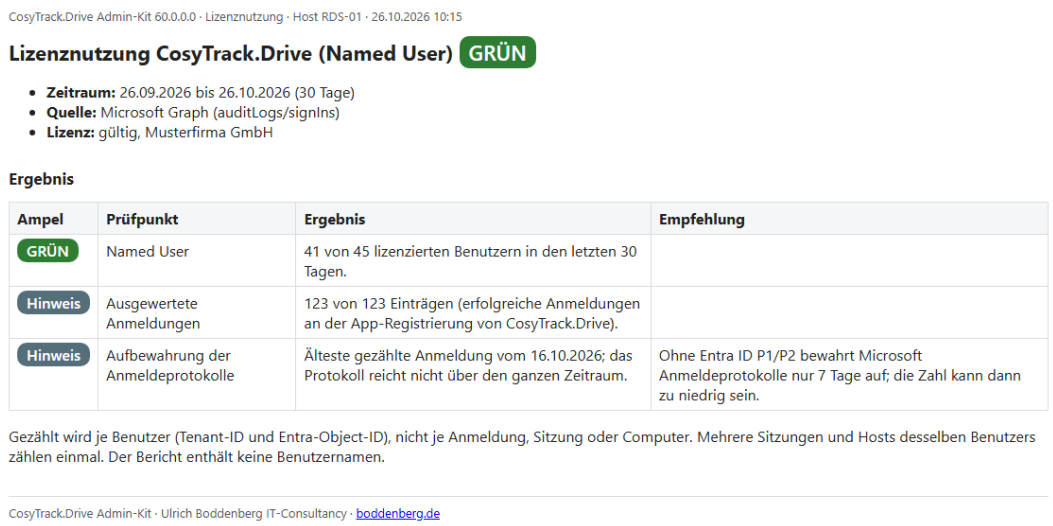


Cache-Ordner, Kontingent pro Benutzer und Haltedauer im Read-Cache stellst du hier ein, im Bild mit Beispielwerten.

Auf Terminalservern, auf denen viele Benutzer denselben Host teilen, gibt es zusätzlich die Richtlinie, den Read-Cache beim Abmelden zu leeren. Ungesendete Änderungen sind davon nie betroffen, sie werden bei der nächsten Anmeldung weiter hochgeladen. Mehr zu Platz, Kontingent und Profilcontainern steht in Cache und Plattenplatz auf dem Terminalserver.

Lizenzbericht und Konfliktkopien

CosyTrack.Drive wird pro Named User lizenziert. Um zu prüfen, ob die Zahl der aktiven Benutzer zur Lizenz passt, liest das Admin-Kit auf Wunsch die Anmeldeprotokolle aus Microsoft Entra ID. Die dafür nötigen Leserechte fordert es nur zur Laufzeit an, sie stehen nicht dauerhaft in der App-Registrierung. Das Ergebnis enthält nur Zahlen, keine Namen. Wie die Zählung im Detail funktioniert, erklärt CosyTrack.Drive lizenzieren: Named User erklärt.



CosyTrack.Drive Admin-Kit 60.0.0.0 · Lizenznutzung · Host RDS-01 · 26.10.2026 10:15

Lizenznutzung CosyTrack.Drive (Named User) GRÜN

- **Zeitraum:** 26.09.2026 bis 26.10.2026 (30 Tage)
- **Quelle:** Microsoft Graph (auditLogs/signIns)
- **Lizenz:** gültig, Musterfirma GmbH

Ergebnis

Ampel	Prüfpunkt	Ergebnis	Empfehlung
GRÜN	Named User	41 von 45 lizenzierten Benutzern in den letzten 30 Tagen.	
Hinweis	Ausgewertete Anmeldungen	123 von 123 Einträgen (erfolgreiche Anmeldungen an der App-Registrierung von CosyTrack.Drive).	
Hinweis	Aufbewahrung der Anmeldeprotokolle	Älteste gezählte Anmeldung vom 16.10.2026; das Protokoll reicht nicht über den ganzen Zeitraum.	Ohne Entra ID P1/P2 bewahrt Microsoft Anmeldeprotokolle nur 7 Tage auf; die Zahl kann dann zu niedrig sein.

Gezählt wird je Benutzer (Tenant-ID und Entra-Object-ID), nicht je Anmeldung, Sitzung oder Computer. Mehrere Sitzungen und Hosts desselben Benutzers zählen einmal. Der Bericht enthält keine Benutzernamen.

CosyTrack.Drive Admin-Kit · Ulrich Boddenberg IT-Consultancy · boddenberg.de

Der Lizenzbericht zeigt mit Demodaten der Musterfirma GmbH nur Anzahlen und Ampel, keine Liste mit Personen.

Ein Detail, das gern übersehen wird, weil es nicht auf dem Rechner, sondern im Tenant liegt: Kann eine Änderung wegen eines Konflikts nicht über die neuere Fassung geschrieben werden, legt CosyTrack.Drive eine Konfliktkopie an. Deren Dateiname enthält den Teil des Anmeldenamens vor dem „@“ oder den Windows-Benutzernamen, damit alle sehen, wessen Fassung das ist. Das ist im Alltag praktisch und sollte in der Beschreibung der Verarbeitung nicht fehlen.

Alles auf einen Blick

Daten	Ort	Personenbezug	Aufbewahrung	Zugriff
Aktivitätsprotokoll	lokal, pro Benutzer	Konto, Anmeldename, Rechner, Pfade	Standard 30 Tage, 200 MB	Benutzer, SYSTEM, Administratoren
Leistungszähler	Arbeitsspeicher	Sitzung und Laufwerk, Namen nur per Richtlinie	nur live, außer mit Datensammler	wer Leistungsindikatoren lesen darf
Ereignisprotokoll	Windows	bereinigt, Ausnahme Administratorhandlungen	nach Windows-Einstellung	nach Windows-Rechten
Diagnosepaket Admin-Kit	lokale Zip-Datei	anonymisiert	bis du es löschst	wer die Datei hat
Diagnosepaket Konfigurations-App	lokale Zip-Datei	Klartext, ohne Tokens	bis du es löschst	nur im eigenen Haus
Read-Cache, Journal, ungesendete Inhalte	lokal, pro Benutzer	Dateiinhalte und Namen	Haltedauer, Kontingent, bis zum Upload	Benutzer, SYSTEM, Administratoren
Lizenznutzung	Bericht im Admin-Kit	nur Zahlen	bis zur nächsten Zählung	Administratoren
Konfliktkopie	SharePoint	Kurzname im	wie andere	wer die Bibliothek

		Dateinamen	Dateien	sieht

Die Betriebs- oder Dienstvereinbarung: Was hineingehört

Eine gute Vereinbarung beschreibt nicht das Produkt, sondern die Nutzung. Sie sagt, wofür Protokolle und Messwerte da sind, wofür ausdrücklich nicht, wer unter welchen Bedingungen hineinschauen darf und wann gelöscht wird. Die Technik liefert dafür die Hebel, die Vereinbarung legt fest, wie sie stehen. Je enger beides zusammenpasst, desto weniger muss später interpretiert werden.



Schematische Darstellung. Die rechte Spalte gehört ausdrücklich in die Vereinbarung, als Verbot.

Zweck festschreiben, Verbote ausdrücklich nennen

Der wichtigste Satz einer solchen Vereinbarung ist der Zweck: Betrieb, Störungsbeseitigung, Kapazitätsplanung und die Nachvollziehbarkeit von Vorgängen auf Bitte der Betroffenen. Ebenso wichtig ist der zweite Satz: Eine Leistungs- oder Verhaltenskontrolle einzelner Personen findet nicht statt. Klingt selbstverständlich, schafft aber Klarheit, wenn in zwei Jahren eine neue Führungskraft fragt, ob man nicht doch mal schauen könne, wer freitags so früh geht.

Regelungspunkte und die passenden technischen Hebel

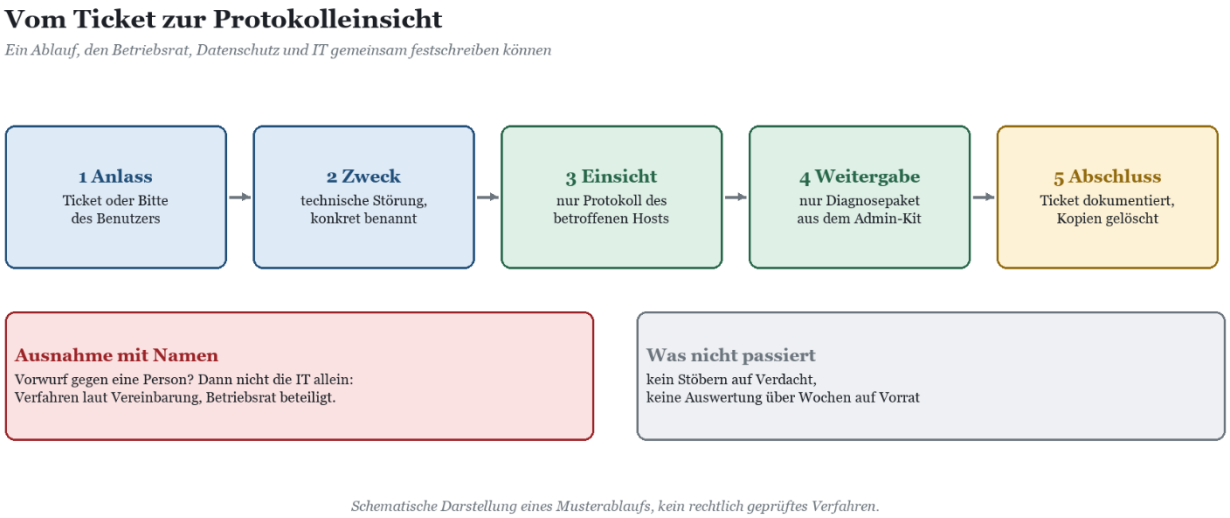
Regelungspunkt	Typischer Vorschlag	Technischer Hebel
Zweck	Betrieb, Fehlersuche, Kapazität, keine Leistungs- oder Verhaltenskontrolle	organisatorisch, in der Vereinbarung
Löschfrist Aktivitätsprotokoll	so kurz wie für die Fehlersuche nötig	Richtlinie „Aufbewahrung des Protokolls“ (Tage, MB)
Ausführliches Protokoll	nur anlassbezogen und befristet	Richtlinie „Ausführliches Protokoll (Debug)“, Standard aus
Leistungszähler ohne Namen	Standard, für Standort- und Hostvergleiche	Instanzen nach Sitzung und Laufwerk
Leistungszähler mit Namen	nicht vorgesehen oder nur mit eigener Regelung	Richtlinie „Benutzernamen in Leistungsindikatoren“, Standard aus
Dauerhafte Aufzeichnung	nur befristet, mit Zweck, Ort und Löschung	Datensammler mit logman oder Überwachungssystem
Weitergabe an Dritte	nur anonymisiert	Diagnosepaket aus dem Admin-Kit

Lokale Kopien	Verschlüsselung der Datenträger, Cache auf Session Hosts leeren	BitLocker, Richtlinie zum Leeren des Read-Caches beim Abmelden
Rollen und Rechte	wer Administrator auf Hosts ist, ist auch Leser der Protokolle	lokale Administratorgruppen, Rollen im Tenant
Änderungen	neue Auswertungen und neue Generationen vorab vorstellen	Änderungsverfahren in der Vereinbarung

Wie du diese Richtlinien zentral setzt, kontrollierst und dokumentierst, beschreibt CosyTrack.Drive per GPO und Intune steuern. Für das Gremium ist ein Ausdruck der gesetzten Werte oft überzeugender als jede Folie, denn er zeigt, was tatsächlich eingestellt ist, nicht was jemand vorhat.

Einsicht ins Protokoll: anlassbezogen, nicht auf Vorrat

Wer darf das Protokoll eines Benutzers lesen, und wann? Bewährt hat sich ein schlichter Ablauf: Es gibt einen Anlass, meist ein Ticket oder die Bitte des Benutzers selbst. Der Zweck ist technisch und konkret. Die Einsicht beschränkt sich auf den betroffenen Rechner oder Sitzungshost und den betroffenen Zeitraum. Was das Haus verlässt, geht als anonymisiertes Diagnosepaket. Am Ende ist das Ticket dokumentiert, und Kopien sind gelöscht.



Schematische Darstellung eines Musterablaufs, kein rechtlich geprüftes Verfahren.

AUS DER PRAXIS · Filialisierter Lebensmittelbetrieb, Montag kurz nach acht

In einer Filiale lässt sich die Bestellliste nicht speichern, die Marktleitung ruft an. Die IT schaut in die Leistungszähler des Terminalservers: Drosselung null, Wartezeit beim Öffnen normal. Im Protokoll der betroffenen Sitzung steht dann der eigentliche Grund, ein hängender Upload wegen eines Dateinamens, den SharePoint nicht mag. Gelöst, bevor der Kaffee kalt war, und ohne dass jemand wissen musste, wer am Wochenende sonst noch gearbeitet hat. So sieht der Zweck in der Praxis aus.

WICHTIG · Der Sonderfall gehört nicht zur IT allein

Steht ein Vorwurf gegen eine bestimmte Person im Raum, etwa ein Verdacht auf Datenabfluss, ist das keine Störung mehr, sondern ein Verfahren. Dann sollte die Vereinbarung festlegen, wer entscheidet und wer beteiligt wird. Die IT liefert auf Anweisung, sie ermittelt nicht auf eigene Faust. Das schützt die Belegschaft und übrigens auch die Administratoren.

Den Betriebsrat früh einbinden, ganz praktisch

Die beste Unterlage für das Gremium ist eine Vorführung. Zeig im Pilot, was das Protokoll enthält, wie das Statusfenster aussieht und was im Leistungsmonitor steht. Zeig die gesetzten Richtlinien. Zeig, dass der Lizenzbericht nur Zahlen hat. Ein Gremium, das die Technik einmal gesehen hat, diskutiert über Regeln statt über Befürchtungen. Wo der Termin im Projektplan hingehört, steht im Einführungsfahrplan für CosyTrack.Drive.

- **Vor dem Pilot:** Projekt vorstellen, Zweck und Datenliste übergeben, Termin für die Vorführung.
- **Im Pilot:** Vorführung von Protokoll, Zählern und Richtlinien, Entwurf der Vereinbarung oder Anlage.
- **Vor dem Rollout:** Vereinbarung abgeschlossen, Richtlinien entsprechend gesetzt, Belegschaft informiert.
- **Im Betrieb:** Änderungen vorab vorstellen, etwa einen neuen Datensammler oder eine neue Generation.

Zur Information der Belegschaft gehört auch die Kurzschulung. Wer weiß, was das Symbol im Infobereich anzeigt und dass das eigene Protokoll nicht in einer Zentrale landet, ist deutlich entspannter. Bausteine dafür findest du in Anwender-Onboarding in einer halben Stunde, und wer Onboarding und Schulung nicht selbst stemmen will, findet passende Formate unter Schulung und Onboarding für CosyTrack.Drive.

FAKTEN · Was auf der Roadmap steht, zählt noch nicht

Geplante Funktionen wie Mehrmandantenfähigkeit, Metadaten-Mapping und Inhaltstypen beim Speichern sind noch nicht verfügbar. Bewertet und vereinbart wird, was installiert ist. Kommt mit einer neuen Version etwas hinzu, das Daten anders verarbeitet, ist das ein Fall für das Änderungsverfahren der Vereinbarung.

FAQ

Ist CosyTrack.Drive mitbestimmungspflichtig?

Das kann dir kein Produktartikel verbindlich beantworten. Technisch gilt: Das Aktivitätsprotokoll enthält Benutzerkonto, Rechner und Pfade, und Leistungszähler können mit Datensammler und Benutzernamen dauerhaft und personenbezogen werden. Damit ist die Eignung zur Überwachung ein Thema. Die sichere Empfehlung ist, Betriebs- oder Personalrat früh zu beteiligen und eine Vereinbarung oder eine Anlage zur bestehenden Vereinbarung abzuschließen.

Sendet CosyTrack.Drive Daten an den Hersteller?

Nein. Der Agent spricht ausschließlich mit der Anmeldung bei Microsoft Entra ID, mit Microsoft Graph und mit SharePoint Online im eigenen Tenant. Es gibt keine Telemetrie an Dritte, und die Lizenz wird offline geprüft.

Wer kann das Protokoll eines Benutzers lesen?

Der Benutzer selbst, SYSTEM und die Administratoren des jeweiligen Rechners oder Sitzungshosts. Das Protokoll liegt lokal im Cache-Verzeichnis des Benutzers und wird nicht zentral gesammelt.

Wie lange wird protokolliert?

Standardmäßig 30 Tage oder bis 200 MB pro Benutzer, je nachdem, was zuerst greift. Beides stellst du mit der Richtlinie „Aufbewahrung des Protokolls“ ein, passend zu der Frist, die ihr vereinbart.

Kann ich mit den Leistungszählern sehen, wie viel einzelne Personen arbeiten?

Standardmäßig nicht, denn die Instanzen heißen nach Sitzung und Laufwerk, und die Werte liegen nur im Speicher. Mit der Richtlinie „Benutzernamen in Leistungsindikatoren“ und einem Datensammler ginge mehr. Genau das ist nicht der Zweck der Zähler und gehört deshalb nur mit einer ausdrücklichen Regelung eingeschaltet, im Normalfall gar nicht.

Darf ich das Diagnosepaket an den Support schicken?

Für die Weitergabe nimmst du das Diagnosepaket aus dem Admin-Kit. Es ersetzt Benutzer, Rechner, Adressen und Pfade durch Zufallswerte und entfernt Tokens. Das Paket aus der Konfigurations-App enthält diese Angaben im Klartext und ist für die Analyse im eigenen Haus gedacht.

Sind die Dateien im Cache verschlüsselt?

Sie sind durch Ordnerrechte geschützt, aber nicht eigens verschlüsselt. Für Verschlüsselung im Ruhezustand setzt du BitLocker auf den Volumes von Cache und Profil ein. Auf Terminalservern kann der Read-Cache zusätzlich beim Abmelden geleert werden.

Brauche ich eine eigene Vereinbarung nur für CosyTrack.Drive?

Nicht unbedingt. Gibt es eine Rahmenvereinbarung zu Microsoft 365 mit Anlagen pro Werkzeug, ist eine neue Anlage oft der schlankeste Weg. Wichtig ist, dass Zweck, Löschfristen, Zugriff und Auswertungsverbote für Protokoll und Leistungszähler konkret geregelt sind.

Fazit: Vertrauen ist gut, Vereinbarung ist besser

Ein Laufwerk auf SharePoint ist eine technische Einrichtung mit Gedächtnis, und das ist kein Makel, sondern Voraussetzung für einen ordentlichen Betrieb. Microsoft 365 protokolliert mit Überwachungsprotokoll, Anmeldeprotokollen und Versionsverlauf bereits eine Menge, mit vernünftigen Voreinstellungen wie verborgenen Namen in den Nutzungsberichten. CosyTrack.Drive ergänzt das um die Sicht vom Rechner aus: ein lokales, befristetes Aktivitätsprotokoll und Leistungszähler ohne Personennamen, ohne Kanal zum Hersteller, alles per GPO oder Intune einstellbar. Damit lassen sich Störungen finden, Standorte vergleichen und Kapazitäten planen, ohne dass irgendwer wissen muss, wer wann Feierabend gemacht hat.

Damit das so bleibt, gehört es aufgeschrieben: in eine Betriebs- oder Dienstvereinbarung, die den Zweck nennt, die Kontrolle ausschließt, Fristen und Zugriffe regelt und Änderungen an ein Verfahren bindet. Das ist weniger Arbeit, als es klingt, und deutlich weniger Arbeit als ein verschobener Rollout. Wenn du Richtlinien, Datenliste und Vorführung für dein Gremium vorbereiten willst, unterstützt dich die Beratung zu CosyTrack.Drive. Fragen zur SharePoint-Struktur und zu Rechten dahinter klärt die SharePoint-Beratung, und Hintergründe rund um die Plattform findest du im Kompetenzbereich SharePoint.

WEITERLESEN · Weiter im Thema

› Microsoft-365-Anbindung messen mit Leistungszählern
› CosyTrack.Drive per GPO und Intune steuern
› Einführungsfahrplan für CosyTrack.Drive
› Cache und Plattenplatz auf dem Terminalserver
› SharePoint als Laufwerk auf dem Terminalserver
› CosyTrack.Drive lizenzieren: Named User erklärt
› Nur lesen oder schreiben: Rechte pro Laufwerk
› Abteilungslaufwerk ablösen ohne Kulturschock
› Onboarding für Systemhäuser