projektmagazin

Veröffentlichungsdatum

2026-02-18

Datenrisiken vermeiden, Transparenz wahren, Effizienz steigern

So gelingt sichere Zusammenarbeit in Projekten

Peter Stoessel

Chief Revenue Officer (CRO)
Tresorit

Management Summary

- Manche eingeübte Arbeitsweise im Projektalltag – etwa Kommunikation über unterschiedliche und uneinheitliche Ablagestrukturen – begünstigt Datenverluste und Sicherheitslücken.
- Unklare Versionsstände und informelle Freigaben erschweren die Nachvollziehbarkeit und können zum Rechtsrisiko werden.
- Entstehen unkoordinierte Einzellösungen außerhalb der IT, können sich daraus unbeabsichtigt Sicherheitsrisiken und Regelverstöße entwickeln.
- Ohne automatische Protokollierung sind Dateiänderungen und Zugriffe oft nicht sichtbar – ein Problem bei Audits und branchenspezifischen Prüfungen.
- Eine digitale Arbeitsumgebung mit klar definierten Rollen, Rechten und Prozessen schafft Transparenz, reduziert Risiken und stärkt die Effizienz der Zusammenarbeit.

Projektstart – und alles scheint geregelt: Das Team ist motiviert, die Tools sind eingerichtet, die Zusammenarbeit läuft. Aber sobald die ersten Deadlines näher rücken, wird es unübersichtlich: Aufgabenlisten liegen im Projekttool, Detailfragen wandern per E-Mail hin und her, Rückfragen landen im Teams-Chat, Entscheidungen werden im nächsten Meeting besprochen – und parallel dazu kursieren unterschiedliche Dateiversionen in verschiedenen Ordnern.

Häufig werden Status-Updates oder Freigaben noch per Hand in Excel-Listen oder Protokolle übertragen. So schleichen sich Fehler ein, Informationen gehen verloren oder bleiben in einzelnen Kanälen "stecken". Viele dieser Arbeitsweisen haben sich im Projektalltag etabliert – mit Nebenwirkungen, die zunächst kaum auffallen.

Die häufigsten Datenrisiken in Projekten

Um ihre Arbeitsabläufe zu vereinfachen, suchen Mitarbeitende oft selbstständig nach Lösungen – und holen damit unbewusst im schlimmsten Fall ein weiteres Problem ins Unternehmen: Schatten-IT. Denn vielversprechend wirkende Tools, die ohne Rücksprache mit der IT-Abteilung genutzt werden, bergen Risiken.

Beispiel aus dem Projektalltag

Oft arbeiten Projektleitungen mit externen Dienstleistern zusammen, die keinen Zugriff auf die interne IT-Infrastruktur haben. Um Dateien schnell und unkompliziert auszutauschen, richten sie eigenständig einen Ordner in einem öffentlichen Cloud-Speicher ein – mit ihrem privaten Account. Nach und nach landen dort nicht nur Präsentationen, sondern auch Verträge, Budgetübersichten und personenbezogene Daten aus dem Projekt.

Die IT-Abteilung weiß nichts von diesem Speicherort, Sicherheits- und Compliance-Vorgaben greifen hier nicht. Wird das Konto kompromittiert oder versehentlich falsch freigegeben, können Unbefugte auf sensible Informationen zugreifen – ohne dass das Unternehmen den Vorfall zunächst bemerkt.

Je komplexer und verteilter die Zusammenarbeit ist, desto wahrscheinlicher sind Stolpersteine. Hier finden Sie **Tipps, wie Sie den vier häufigsten Sicherheitsrisiken im Projekt begegnen:** unklare Versionen und Freigabeprozesse, Tool-Wildwuchs, fehlende Nachvollziehbarkeit und fehlende Governance. Zusätzlich erzielen Sie mit den empfohlenen **Quick Wins** – kleinen, sofort wirksamen Maßnahmen – ohne größeren Aufwand positive Effekte bei der Datensicherheit.

Risiko 1: Unklare Versionen und Freigabeprozesse

Fehlt ein klares System für Versionen und Freigaben, wird Projektarbeit schnell unübersichtlich. Dateien werden dann häufig mehrfach bearbeitet und parallel geteilt, Freigaben erfolgen spontan per E-Mail oder Zuruf. Sind mehrere Dokumentstände gleichzeitig im Umlauf – in Cloud-Ordnern, per E-Mail oder lokal auf Geräten –, führt das zu Inkonsistenzen, Mehraufwand und im schlimmsten Fall zu Entscheidungen auf Basis veralteter Informationen.

Besonders in stark regulierten Branchen können unklare Freigabeprozesse zum Risiko werden: Ohne eindeutige Nachweise lässt sich nicht belegen, wer wann welche Version geprüft oder freigegeben hat. Auch in allen anderen vertraglich geregelten Projekten für externe Kunden stellen unklare Freigabeprozesse ein Haftungsrisiko dar.

Tipp: Eine Plattform mit zentraler, einheitlicher Datenbasis (auch als "Single Source of Truth" bezeichnet) verringert Mehrfachspeicherungen deutlich und ermöglicht digitale Prüfschritte durch Rollen- und Rechtezuweisungen.

Quick Wins

- **Eine zentrale Ablage einführen**, z.B. einen gemeinsamen Projektordner mit klarer Struktur, eindeutigen Verantwortlichkeiten und definierten Sicherheitsvorgaben. Wichtig: Für Datensicherheit braucht es eine transparente Kommunikation mit der IT, ob Lösungen den geltenden Datenschutz- und Compliance-Anforderungen entsprechen. Zugriffsrechte nach Rollen und verschlüsselte Speicherorte tragen positiv zu klaren Freigabeprozessen bei.
- **Mit Versionen arbeiten**: Versionierung aktivieren oder Benennungssystem einführen ("v1", "final", "final_approved")
- **Alte Dateien archivieren** statt löschen – so bleibt die Historie nachvollziehbar
- **Freigaben dokumentieren**: im Projektboard, Protokoll oder direkt im Dokument

Risiko 2: Tool-Wildwuchs

Unkoordinierte Einzellösungen

Pragmatische Lösungen sind prinzipiell etwas Gutes. Doch sie werden zur Gefahr, wenn unterschiedliche Teams unterschiedliche Tools nutzen – intern wie extern. Unternehmen sollten daher die Wünsche ihrer Mitarbeitenden nach digitaler Unterstützung ernst nehmen und gezielt umsetzen. Andernfalls suchen Teams selbst nach Lösungen und umgehen die IT bei der Einführung. Projektleitende sind hier in der Pflicht: Sie tragen dem Unternehmen gegenüber Verantwortung für eine regelkonforme Toolnutzung.

Fehlen standardmäßig Verschlüsselung, klar definierte Zugriffsrechte und eine zentrale Administration, steigt das Risiko für Datenabfluss deutlich. Das gilt auch, wenn organisatorische Sicherheit durch ausbleibende Mitarbeiterschulungen oder intransparente Prozesse nicht vollständig gewährleistet ist. Dann können sich Unbefugte leichter Zugriff verschaffen, Accounts gehackt oder Links versehentlich zu weit geteilt werden. So werden aus pragmatischen Einzellösungen schnell reale Sicherheitsrisiken für die Organisation.

E-Signaturen ohne zentrale Nachvollziehbarkeit

Sicherheitslücken entstehen im Arbeitsalltag auch dann, wenn Teams separate, nicht in die Unternehmens-IT integrierte E-Signatur-Tools nutzen. Statt Prozesse zu vereinfachen, entstehen dadurch neue Sicherheitsrisiken, weil sensible Daten außerhalb der geschützten Projektumgebung verarbeitet werden.

Kritisch wird es insbesondere dann, wenn im Projektverlauf mehrere Verträge oder Freigaben über verschiedene E-Signatur-Lösungen laufen: Im Auditfall lässt sich kaum noch zweifelsfrei nachvollziehen,

welche Person welche Version eines Dokuments wann freigegeben hat – oder ob vertrauliche Inhalte versehentlich in einem nicht autorisierten System gelandet sind.

Tipp: Kommunikation, Datenaustausch und Freigaben – auch per E-Signatur – sollten möglichst über eine Plattform erfolgen. Eine Ist-Analyse zeigt, ob im Unternehmen bereits eine Lösung vorhanden ist, die diese Anforderungen abdeckt.

Quick Wins

- **Tool-Inventur machen**: Welche Softwaretools haben wir, wo werden vertrauliche Daten ausgetauscht? Überflüssige oder doppelte Lösungen anschließend stilllegen.
- Beim **Datenaustausch mit externen Partnern** klar definieren und kommunizieren, welche Plattform für die Zusammenarbeit genutzt wird.

Risiko 3: Fehlende Nachvollziehbarkeit

Mangelnde Transparenz darüber, wer wann welche Datei bearbeitet, geteilt oder freigegeben hat, erzeugt schnell Unsicherheit – im Projektalltag ebenso wie im Auditfall. Gerade bei Prüfungen, etwa im Rahmen von ISO-, NIS2- oder Datenschutz-Audits, müssen Projektverantwortliche in Zusammenarbeit mit der Unternehmens-IT nachweisen können, welche Informationen zu welchem Zeitpunkt vorlagen und wer welche Freigabe erteilt hat.

Was ist die NIS2-Richtlinie?

NIS steht für "Network and Information Security". Die NIS2-Richtlinie ist eine EU-weite Vorgabe zur Verbesserung der Cyber- und Informationssicherheit. Sie verpflichtet bestimmte Unternehmen und Organisationen dazu, angemessene technische und organisatorische Sicherheitsmaßnahmen umzusetzen. Dazu gehören u.a. Risikomanagement, der Schutz sensibler Daten gegen Angriffe und klare Prozesse für den Umgang mit Sicherheitsvorfällen. Ziel ist es, Ausfälle und Datenpannen zu reduzieren und die Widerstandsfähigkeit kritischer Dienste in Europa zu stärken.

Fehlt ein durchgängiges Logging, also die automatische Protokollierung aller wichtigen Aktionen, lassen sich Änderungen und Zugriffe nicht lückenlos nachvollziehen. Verantwortlichkeiten bleiben unklar, insbesondere dann, wenn Teams in unterschiedlichen Tools ohne gemeinsame Protokollierung arbeiten. Wird eine Datei versehentlich geändert oder gelöscht, fehlt oft der Nachweis, wer dafür verantwortlich war – oder ob sensible Daten unbefugt eingesehen wurden.

Tipp: Organisationen sollten auf Systeme mit automatisiertem Logging und auf klare Regeln zum Umgang damit setzen. So lassen sich Änderungen und Zugriffe transparent dokumentieren und Anforderungen aus ISO-, NIS2- oder branchenspezifischen Prüfungen zuverlässig erfüllen.

Quick Wins

- **Logging-Funktionen** in bestehenden Systemen aktivieren
- **Änderungsprotokolle** regelmäßig exportieren oder sichern
- **Zugriffsrechte** zentral verwalten und regelmäßig prüfen

Risiko 4: Fehlende Governance

Schattenprozesse und unklare Verantwortlichkeiten sind in jedem Projekt zu vermeiden. Dafür braucht es Governance. Fehlt diese Klammer aus klaren Regeln und Zuständigkeiten, werden viele der zuvor beschriebenen Probleme überhaupt erst möglich. Ohne definierte Regeln, wer welche Daten nutzt, freigibt oder speichert, entwickeln sich Abläufe nach individuellen Vorlieben – und damit außerhalb zentraler Richtlinien.

Was bedeutet Governance im Projektkontext?

Governance beschreibt, wie Projekte geführt werden. Sie legt fest, wer wofür Verantwortung trägt, wie Entscheidungen zustande kommen und wie der Umgang mit Informationen und Freigaben geregelt ist. Eine funktionierende Projekt-Governance verhindert, dass Projekte durch informelle Absprachen oder uneinheitliche Vorgehensweisen aus dem Ruder laufen.

Teams passen bestehende Prozesse eigenständig an, um Zeit zu sparen oder pragmatische Lösungen zu finden. Auf diese Weise entstehen parallele Workflows und Unklarheiten in den Zuständigkeiten. Das ist besonders kritisch, wenn sensible Informationen betroffen sind.

Tipp: Governance ist die Grundlage für Auditierbarkeit – sie definiert, was Teams dokumentieren müssen und wer für die Einhaltung verantwortlich ist. Klare Richtlinien sollten festlegen, über welche Kanäle Projektteams Daten austauschen (z.B. nur über die freigegebene Projektplattform statt über private Cloud-Speicher), wer Dokumente in welcher Rolle bearbeiten und freigeben darf und wo diese Schritte dokumentiert werden – etwa im Projektboard oder direkt im Tool.

Quick Wins

- **Rollen und Verantwortlichkeiten** pro Projekt eindeutig festlegen
- Kurze **Governance-Checkliste** für neue Tools oder Prozesse einführen
- Regelmäßige **Kurzreviews** etablieren, z.B. **"Governance Health Checks"**. Hier können Teams überprüfen, ob die vereinbarten Tools genutzt werden, Zugriffsrechte weiterhin passen, Freigabewege eingehalten werden und ob sich in der Praxis Schattenprozesse oder neue Dateninseln gebildet haben. So bleibt Governance kein einmaliges Konzept, sondern wird regelmäßig im Projektalltag überprüft.

Eine gemeinsame Arbeitsumgebung für sichere Projektarbeit

Die vier beschriebenen Risiken zeigen: Unklare Versionen, intransparente Freigaben oder Schattenprozesse können zu ineffizienter Projektarbeit führen und gefährden den sicheren Umgang mit Daten. Zugleich wird deutlich, dass Datenprobleme selten isoliert auftreten, sondern Symptome fehlender Strukturen und Verantwortlichkeiten sind.

Um die Zusammenarbeit effizient zu gestalten und sensible Daten zuverlässig zu schützen, braucht es eine einheitliche Arbeitsumgebung – also einen klar definierten Rahmen, in dem Projektteams Daten ablegen, bearbeiten und freigeben können –, ergänzt durch klare Regeln und Transparenz über alle Projektphasen hinweg. Digitale Strukturen bilden hierfür meist die effizienteste Basis. Je nach Projektgröße, Branche und der zugrundeliegenden Organisationsstruktur sind verschiedene integrierte Kollaborationsplattformen denkbar. Bewährt haben sich unter anderem projektfähige Datenräume.

Klassische Datenräume sind den meisten Projektverantwortlichen ein Begriff. Ihr Fokus lag bislang auf einmaligen Datenübermittlungen. Projektfähige Datenräume gehen einen Schritt weiter: Sie ermöglichen dank strukturierter, berechtigungsgesteuerter Arbeitsbereiche eine langfristige, sichere Zusammenarbeit über den gesamten Projektverlauf hinweg.

Damit eine Arbeitsumgebung den Anforderungen moderner Projektarbeit gerecht wird, sollte sie mindestens die folgenden sechs Kriterien erfüllen:

- **Sicherheit**: Schutz sensibler Inhalte, Ende-zu-Ende-Verschlüsselung, Unterstützung von Compliance-Anforderungen
- **Flexibilität**: Orts- und zeitunabhängige Zusammenarbeit mit internen und externen Partnern
- **Nachvollziehbarkeit**: Lückenlose Dokumentation aller Änderungen, Zugriffe und Freigaben

- **Verbindlichkeit**: Rechtssichere digitale Signaturen und klar definierte Rollen
- **Benutzerfreundlichkeit**: Intuitive Bedienung, geringe Einstiegshürden, insbesondere für Externe
- **Rollen und Rechte**: Ob Projektmanager:innen, IT-Verantwortliche oder Projektleitung – unterschiedliche Rollen benötigen unterschiedliche Rechte. Für maximale Sicherheit sollten Unternehmen konsequent auf das Least-Privilege-Prinzip setzen: Jede Person erhält nur die Rechte, die sie für ihre Aufgaben benötigt.

Damit wird deutlich: Ob es um Versionen, Tools, Nachvollziehbarkeit oder Governance geht – letztlich dreht sich alles um die Frage, wie Projekte organisiert sind. Wer eine gemeinsame Arbeitsumgebung schafft, Verantwortlichkeiten klar regelt und Datenflüsse transparent hält, reduziert nicht nur Sicherheitsrisiken, sondern vereinfacht auch den Projektalltag für alle Beteiligten.

Fazit: Struktur schafft Sicherheit – und Effizienz

Der erste Schritt zu einer erfolgreichen Zusammenarbeit besteht darin, sich von manuellen Abläufen, aufwendigen Abstimmungen und einer unübersichtlichen Dateiablage zu lösen. Klare Prozesse und digitale Strukturen helfen dabei, Aufgaben nachvollziehbar sowie effizient zu gestalten, und stärken zugleich die Datensicherheit.

Denn gerade in Projekten gilt: Wer seine Daten fest im Griff hat, behält auch die Kontrolle über seine Projekte und schafft so die Grundlage für eine vertrauensvolle Zusammenarbeit zwischen Teams, Auftraggebern und Partnern. Schließlich bilden Daten das Fundament des Vertrauens und verdienen entsprechenden höchsten Schutz. (kt)