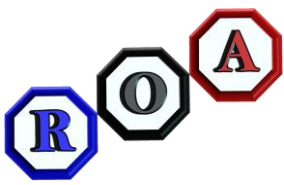




Power Apps Governance: Sicherheit als Motor der Freiheit

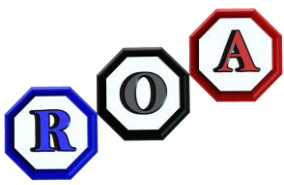
„Wer hat Zugriff auf diese Daten?“ – Wie Sie 2026 die Kontrolle behalten, ohne Innovationen zu blockieren.

Ein Whitepaper von Volker Buntrock



Inhaltsverzeichnis

Executive Summary	2
Einleitung: Das nächtliche Gedankenkarussell der IT-Leitung.....	3
Die Illusion der Sicherheit durch Verbote	5
Die neue Balance - Ermöglichen innerhalb sicherer Grenzen.....	6
Die technische Rüstung - DLP und das Admin Center als Kontrollinstanzen	8
Die Umgebungs-Strategie - Vom Sandkasten zur geschäftskritischen Lösung	10
Der Mensch im Mittelpunkt - Das Center of Excellence (CoE).....	12
Fazit - Sicherheit schafft die Freiheit zum Sieg.....	14



Executive Summary

Problem:

Die unkontrollierte Nutzung von Low-Code-Tools wie Power Apps führt in vielen Unternehmen zu einem massiven Kontrollverlust der IT. Fachabteilungen erstellen eigenständig Apps, die potenziell sensible Daten verarbeiten, ohne dass die IT weiß, *wer* Zugriff hat, *welche* Konnektoren genutzt werden oder *wohin* Daten abfließen. Verbote schaffen nur Schatten-IT und erhöhen das Risiko von Datenlecks, Compliance-Verstößen und instabilen, ungewarteten Anwendungen.

Lösung:

Eine moderne Power-Platform-Governance ersetzt Verbote durch transparente, sichere Leitplanken. Sie besteht aus DLP-Richtlinien, einer klaren Umgebungsstrategie (Sandbox → Test → Produktion), zentraler Kontrolle über das Power Platform Admin Center und einem Center of Excellence (CoE), das Schulungen, Standards und automatisierte Governance bereitstellt. So entsteht eine „Managed Freedom“, in der Fachbereiche schnell digitalisieren können, ohne die Sicherheit zu gefährden.

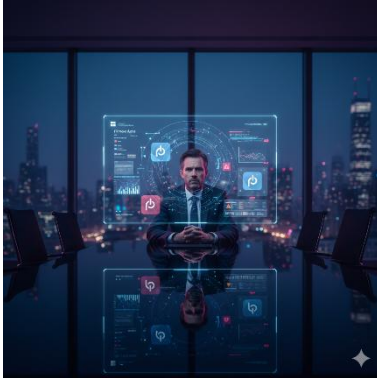
Mehrwert:

Die IT gewinnt volle Sichtbarkeit, stabile Sicherheitsmechanismen und planbare Skalierung. Fachbereiche profitieren von kreativer Freiheit, klaren Standards und einer offiziellen Plattform, die Innovation ermöglicht, ohne Risiken zu erzeugen. Das Unternehmen erhält sichere, geprüfte, reproduzierbare Apps statt unkontrollierter Einzellösungen – und die IT-Leitung kann wieder ruhig schlafen.

Risiko ohne Governance:

Ohne professionelle Leitplanken entstehen Schatten-IT, Datenlecks, DSGVO-Verstöße, unkontrollierte Konnektoren, instabile Apps und organisatorische Abhängigkeiten von Einzelentwicklern. Stillstand und Sicherheitsrisiken werden wahrscheinlicher als Innovation – und jede neue App kann potenziell ein unkalkulierbares Risiko darstellen.

Einleitung: Das nächtliche Gedankenkarussell der IT-Leitung



„Wer hat Zugriff auf diese Daten?“

Es ist keine einfache Frage. Für einen IT-Leiter ist es oft die Frage, die den Unterschied zwischen einem ruhigen Feierabend und einer schlaflosen Nacht ausmacht. In einer Welt, in der Daten das wertvollste Gut eines Unternehmens sind, wirkt die unkontrollierte

Ausbreitung von Applikationen wie ein schleichender Kontrollverlust.

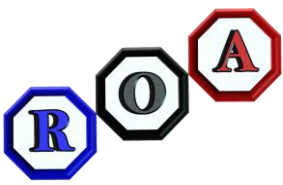
Das Gedankenkarussell beginnt sich zu drehen: Wurden Berechtigungen korrekt vergeben? Fließen sensible Informationen über unsichere Schnittstellen nach außen? Entsteht gerade irgendwo im Marketing oder Vertrieb eine App, von der wir erst erfahren, wenn es zu spät ist?

In den Fluren der IT-Abteilungen herrscht oft eine verständliche Skepsis. Wenn Fachabteilungen - getrieben von echtem Innovationsgeist und dem Wunsch nach Effizienz - anfangen, mit Low-Code-Werkzeugen eigene Lösungen zu bauen, läuten die Alarmglocken. Und das zu Recht. Das Risiko von Datenlecks, instabilen Verbindungen zu kritischen Kernsystemen und handfesten DSGVO-Verstößen ist in Zeiten von Citizen Development realer denn je. Ein einziger falsch konfigurierter Konnektor kann theoretisch ausreichen, um interne Datenbanken für die Außenwelt zu öffnen.

Doch hier liegt das Paradoxon der modernen Digitalisierung: Wer heute Innovation durch strikte Verbote blockiert, schützt zwar kurzfristig die Infrastruktur, gefährdet aber langfristig die Wettbewerbsfähigkeit des gesamten Unternehmens. Die Fachbereiche warten nicht mehr monatelang auf die Kapazitäten der IT; sie suchen sich eigene Wege. Die Zeiten, in denen die IT als „Abteilung für Nein“ fungierte, sind unwiderruflich vorbei.

©2026 Volker Buntrock - alle Rechte vorbehalten!

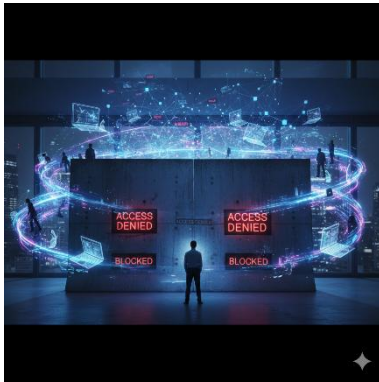
97D Horninglow Road North . Burton-upon-Trent . DE13 0SR . United Kingdom
E-Mail: roa@rohinie.com . Internet: <https://rohinie.com> VAT No. GB498194138



Power Apps Governance: Sicherheit als Motor der Freiheit

Wir stehen vor einer neuen Herausforderung: Wie schaffen wir eine Balance, die den Fachbereichen die kreative Freiheit lässt, ihre Prozesse eigenständig zu digitalisieren, während die IT die Zügel der Sicherheit und Governance fest in der Hand behält? Es geht im Jahr 2026 nicht mehr um „Verhindern“, sondern um „Ermöglichen innerhalb sicherer Leitplanken“. Wir müssen das Gedankenkarussell stoppen - nicht durch das Anhalten der Innovation, sondern durch ein Fundament, auf dem man wieder ruhig schlafen kann.

Die Illusion der Sicherheit durch Verbote



In der Vergangenheit war die Welt der IT-Sicherheit oft binär: Erlaubt oder Verboten. Es gab die geschlossene Festung des Unternehmensnetzwerks, und alles, was außerhalb dieser Mauern stattfand, wurde als Bedrohung eingestuft. Doch diese Strategie der „harten Hand“ stößt in der modernen Arbeitswelt an ihre Grenzen. Wer heute versucht, Low-Code-Plattformen wie Power

Apps pauschal zu sperren, erzeugt oft genau das, was er eigentlich verhindern will: Schatten-IT.

Wenn Fachbereiche unter hohem Zeitdruck stehen und die zentrale IT-Abteilung aufgrund von Personalmangel oder Priorisierung eine Wartezeit von sechs bis zwölf Monaten für eine kleine Prozessoptimierung veranschlagt, suchen sich die Mitarbeiter alternative Wege. Anstatt eine offizielle, sichere Plattform zu nutzen, werden dann unkontrollierte Drittanbieter-Tools, private Cloud-Speicher oder komplexe, fehleranfällige Excel-Konstrukte verwendet.

Das Ergebnis ist eine **Pseudo-Sicherheit**. Während die IT glaubt, die volle Kontrolle zu haben, entstehen im Hintergrund Dateninseln, auf die niemand Zugriff hat und die bei einem Audit oder einem Sicherheitsvorfall zum Disaster führen. Die Illusion, dass ein Verbot das Problem löst, ist gefährlich. Ein Verbot verhindert nicht den Bedarf an Digitalisierung – es drängt ihn nur in den Untergrund.

Echte Sicherheit entsteht nicht durch Mauern, sondern durch Sichtbarkeit. Wenn wir den Mitarbeitern eine offizielle, sanktionierte Plattform wie die Power Plattform zur Verfügung stellen, holen wir die Innovation zurück in das Sichtfeld der IT. Wir müssen verstehen, dass der Wunsch der Fachabteilungen nach Eigeninitiative kein Angriff auf die IT-Souveränität ist, sondern ein Zeichen von Agilität. Die Aufgabe der IT im Jahr 2026 ist es daher, nicht mehr der Torwächter zu sein, der den Weg versperrt, sondern der Architekt, der die sichere Straße baut.

Die neue Balance – Ermöglichen innerhalb sicherer Grenzen



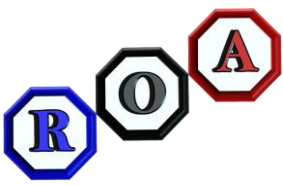
Wenn wir akzeptieren, dass Verbote keine Lösung sind, stellt sich die entscheidende Frage: Wie sieht die Alternative aus? Die Antwort liegt in einem Paradigmenwechsel. Wir bewegen uns weg von einer reaktiven Kontrolle hin zu einer proaktiven Gestaltung. Governance bedeutet heute nicht mehr „Überwachung“, sondern das Setzen von **Leitplanken**.

Stellen Sie sich eine Autobahn vor: Die Leitplanken verhindern nicht, dass Sie schnell fahren oder Ihr Ziel erreichen. Sie sorgen lediglich dafür, dass Sie im Falle eines Fehlers nicht von der Fahrbahn abkommen und sich oder andere gefährden. Genau das leistet eine moderne Power Apps Governance für Ihr Unternehmen.

Diese neue Balance basiert auf drei strategischen Säulen:

1. **Transparenz statt Misstrauen:** Die IT erhält vollständige Sichtbarkeit über alle erstellten Applikationen, genutzten Konnektoren und aktiven Nutzer. Nichts geschieht mehr im Verborgenen. Diese Transparenz ist die Voraussetzung für Vertrauen.
2. **Skalierbare Sicherheit:** Anstatt jede einzelne App manuell zu prüfen (was bei der Geschwindigkeit von Low-Code unmöglich ist), definieren wir globale Regeln. Diese Regeln greifen automatisch, egal ob eine oder tausend Apps erstellt werden.
3. **Befähigung des Einzelnen:** Der Citizen Developer wird nicht als Risiko gesehen, sondern als wertvolle Ressource. Innerhalb der sicheren Leitplanken darf – und soll – er kreativ sein. Die IT definiert den Raum, der Fachbereich füllt ihn mit Leben.

Das Ziel dieser Balance ist eine „Managed Freedom“. Ein Zustand, in dem der Fachbereich das Gefühl hat, autonom und schnell agieren zu können, während der IT-Leiter die Gewissheit hat, dass keine Applikation die Compliance-Regeln des Unternehmens verletzen kann.



Power Apps Governance: Sicherheit als Motor der Freiheit

Governance ist somit kein Bremsklotz, sondern das Schmiermittel für eine sichere, digitale Transformation. Wir schaffen ein Umfeld, in dem Innovation nicht auf Kosten der Sicherheit geht, sondern durch sie erst ermöglicht wird.

Die technische Rüstung – DLP und das Admin Center als Kontrollinstanzen



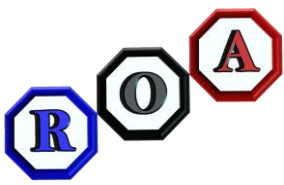
Konzepte und Philosophien sind wichtig, doch am Ende des Tages braucht ein IT-Leiter handfeste Werkzeuge, auf die er sich verlassen kann. Innerhalb der Microsoft Power Platform ist die technische Rüstung für diese Aufgabe zweigeteilt: Es geht um das **Wissen** (Sichtbarkeit) und das **Reglementieren** (Schutz).

Die **Data Loss Prevention (DLP) Policies** sind dabei das schärfste Schwert. Oft herrscht die Angst vor, dass ein unerfahrener Anwender sensible Kundendaten aus einem SQL-Server oder dem SAP-System nimmt und sie – vielleicht sogar unbewusst – über einen Standard-Konnektor mit sozialen Netzwerken oder unsicheren Cloud-Speichern teilt. Mit DLP-Richtlinien unterbinden wir dieses Risiko im Keim. Wir klassifizieren Konnektoren in Gruppen wie „Business“, „Non-Business“ und „Blocked“. Ein Datenaustausch zwischen diesen Welten wird systemseitig technisch verhindert. So kann die IT sicherstellen, dass Unternehmensdaten dort bleiben, wo sie hingehören, während private Tools strikt getrennt bleiben.

Die zweite Komponente ist das **Power Platform Admin Center**. Es ist das Cockpit, in dem alle Fäden zusammenlaufen. Hier wird die Governance zentralisiert, statt sie mühsam in Einzellösungen zu suchen. Die IT behält jederzeit den Überblick:

- Welche Umgebungen existieren in unserem Tenant?
- Wer hat die Berechtigung, Apps zu erstellen oder zu teilen?
- Welche Konnektoren werden in welcher App tatsächlich genutzt?

Diese zentrale Verwaltung ermöglicht es, Anomalien frühzeitig zu erkennen. Wenn plötzlich eine App eine ungewöhnlich hohe Nutzerzahl aufweist, kann die IT proaktiv das Gespräch mit dem Fachbereich suchen, um die Skalierung und Sicherheit gemeinsam zu bewerten.



Power Apps Governance: Sicherheit als Motor der Freiheit

Das Admin Center verwandelt die IT von einer reaktiven Feuerwehr in einen vorausschauenden Fluglotsen. Durch diese technische Tiefe wird die eingangs erwähnte „Sichtbarkeit“ zur harten Währung für die Sicherheit des gesamten Unternehmens.

Die Umgebungs-Strategie – Vom Sandkasten zur geschäftskritischen Lösung

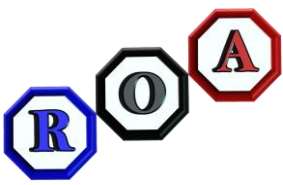


Ein häufiger Albtraum für IT-Abteilungen ist die Vorstellung, dass eine im Fachbereich „gebastelte“ Applikation plötzlich zum Rückgrat eines wichtigen Geschäftsprozesses wird, ohne jemals auf Stabilität, Skalierbarkeit oder Sicherheit geprüft worden zu sein. Wenn diese App dann am Montagmorgen ausfällt, landet das Problem unweigerlich auf dem Tisch der IT.

Um dieses Szenario zu verhindern, setzen wir auf eine klare **Umgebungs-Strategie**. Wir trennen die Spielwiese strikt von der Werkbank und der Fabrikhalle.

1. **Die Sandbox (Der Sandkasten):** Hier dürfen Citizen Developer experimentieren. Es ist ein abgeschirmter Bereich, in dem keine Verbindung zu produktiven Kundendaten besteht. Hier kann nichts „kaputtgehen“. Es ist der Ort, an dem Innovation ohne Risiko stattfindet.
2. **Die Test-Umgebung:** Sobald eine App einen Mehrwert verspricht, zieht sie in die Test-Umgebung um. Hier wird geprüft: Funktioniert die Logik? Sind die Schnittstellen stabil? Entspricht das Design den Unternehmensvorgaben?
3. **Die Produktions-Umgebung:** Erst nach einem erfolgreichen Check – idealerweise unterstützt durch automatisierte Pipelines oder ein kurzes Review – geht die App „live“. Nur hier hat sie Zugriff auf die echten, produktiven Datenquellen.

Diese Trennung hat einen entscheidenden Vorteil für den IT-Leiter: Er weiß genau, welche Applikationen „unter dem Radar“ laufen und welche den Status einer geschäftskritischen Anwendung erreicht haben. Apps in der Produktion unterliegen strengeren Governance-Regeln und einem professionellen Monitoring.



Power Apps Governance: Sicherheit als Motor der Freiheit

Durch dieses Stufenmodell verhindern wir das „Wild-West-Szenario“. Wir geben dem Fachbereich den Raum zum Ausprobieren, stellen aber sicher, dass nur das, was wirklich Hand und Fuß hat, den Weg in den operativen Alltag findet. Es ist der Übergang vom individuellen Tool zur stabilen Unternehmenslösung – kontrolliert, dokumentiert und sicher.

Der Mensch im Mittelpunkt – Das Center of Excellence (CoE)



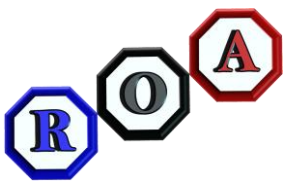
Selbst wenn die theoretischen Leitplanken stehen, scheitert die Umsetzung in der Praxis oft an einer banalen Ressource: Zeit. Eine IT-Abteilung, die bereits mit dem Tagesgeschäft und geschäftskritischen Infrastrukturprojekten voll ausgelastet ist, kann nicht jede Citizen-Developer-App im Detail prüfen. Hier wird ein dediziertes Sicherheitsnetz notwendig, das als dauerhafte Brücke zwischen den Welten

fungiert.

Dieses Sicherheitsnetz basiert auf einem strukturierten Rahmenwerk, das die IT-Leitung entlastet, ohne die Kontrolle abzugeben:

1. **Kontinuierliche Audits:** Governance ist kein statischer Zustand, sondern ein Prozess. Durch regelmäßige Prüfzyklen werden bestehende Apps auf Best Practices, Performance und Sicherheitslücken untersucht. So wird verhindert, dass aus agilen Lösungen über die Zeit instabile „Legacy-Systeme“ werden.
2. **Framework-Pflege:** Die technologische Landschaft der Power Platform entwickelt sich rasant. Ein stabiles Sicherheitsnetz sorgt dafür, dass die internen Richtlinien (DLP, Umgebungs-Strategien) stets auf dem neuesten Stand bleiben und an neue Anforderungen der Fachbereiche angepasst werden.
3. **Qualitätssicherung und Experten-Support:** Wenn Citizen Developer an komplexe Grenzen stoßen, bedarf es einer Instanz, die fachlich unterstützt, dabei aber die Compliance-Regeln des Unternehmens nie aus den Augen verliert. Dies stellt sicher, dass Lösungen nicht nur „irgendwie funktionieren“, sondern professionellen Standards entsprechen.

Dieses Modell der begleiteten Governance verwandelt das Risiko unkontrollierter Eigenentwicklungen in ein stabiles Innovations-Ökosystem.



Power Apps Governance: Sicherheit als Motor der Freiheit

Es ist die Antwort auf die Frage, wie ein mittelständisches Unternehmen Agilität leben kann, ohne die IT-Sicherheit durch personelle Engpässe zu gefährden.

Fazit – Sicherheit schafft die Freiheit zum Sieg



Wir kehren zurück zur Ausgangsfrage: „Wer hat Zugriff auf diese Daten?“

Am Ende dieses Leitfadens sollte diese Frage keinen Alarmzustand mehr auslösen, sondern die Souveränität einer gut geführten IT widerspiegeln. Governance in der Power Platform ist kein notwendiges Übel und kein bürokratisches Hindernis. Sie ist das

Fundament, auf dem echte digitale Transformation erst entstehen kann.

Ohne Kontrolle herrscht Chaos – und Chaos ist der natürliche Feind jeder Skalierung. Doch ohne Freiheit herrscht Stillstand – und Stillstand ist das Ende der Wettbewerbsfähigkeit. Die moderne IT-Leitung im Jahr 2026 hat verstanden, dass ihre Rolle darin besteht, den Raum zwischen diesen beiden Extremen zu gestalten.

Durch den Einsatz von **DLP-Richtlinien**, einer durchdachten **Umgebungs-Strategie** und dem Aufbau einer **Kultur der Befähigung** (wie im CoE-Ansatz beschrieben) verwandeln Sie die Power Platform von einer potenziellen Gefahrenquelle in einen strategischen Motor. Sie bieten Ihren Fachbereichen die Freiheit, Lösungen in Lichtgeschwindigkeit zu entwickeln, während Sie im Hintergrund die Gewissheit haben, dass das „Schloss“ am digitalen Tresor sicher verriegelt bleibt.

Sicherheit ist nicht der Gegenspieler der Freiheit, sondern ihre Voraussetzung. Wer die Leitplanken präzise setzt, kann es sich leisten, das Tempo zu erhöhen. So wird aus dem nächtlichen Gedankenkarussell eine klare Vision: Eine Organisation, die agil genug ist, um sich selbst zu digitalisieren, und sicher genug, um dabei niemals die Kontrolle zu verlieren.