FIKTIVES BEISPIEL

Einkaufsagent bei einem Maschinenbauer

Firma: Huber Präzisionsteile GmbH, 180 Mitarbeiter, Schwaben.

Ausgangslage

Der Einkauf bestellt täglich Normteile, Schrauben und Verbrauchsmaterial bei rund 40 Lieferanten. Zwei Mitarbeiterinnen verbringen einen Großteil ihrer Zeit mit Preisvergleichen und Routinebestellungen. Ein KI-Agent soll das übernehmen. Die Geschäftsführung fürchtet, dass der Agent zu teuer, zu viel oder beim falschen Lieferanten bestellt.

Einsatz von MolTrust

Der Einkaufsagent erhält eine eigene Identität (DID). Die Einkaufsleiterin erteilt ihm eine Vollmacht im AAE-Format: nur freigegebene Lieferanten, höchstens 2.000 € pro Bestellung, höchstens 15.000 € pro Woche, nur Warengruppen C-Teile. Vor jeder Bestellung prüft MolTrust, ob die Bestellung in diese Vollmacht passt. Alles außerhalb wird blockiert und an einen Mitarbeiter weitergeleitet.

Nutzen

- Routinebestellungen laufen rund um die Uhr ohne manuelles Zutun.
- Die Mitarbeiterinnen kümmern sich um Lieferantenverhandlungen und Engpässe.
- Jede Bestellung ist nachträglich prüfbar: wer hat was erlaubt, welche Regel galt.
- Lieferanten können ihrerseits prüfen, dass der Agent im Namen von Huber bestellen darf.

> Die Firmen in diesen Beispielen sind erfunden. Die Abläufe zeigen, wie MolTrust in einem mittelständischen Betrieb eingesetzt werden kann.

Integration durch die IT

1. Konto bei MolTrust anlegen, Organisation registrieren.
2. Für den Einkaufsagenten eine DID erzeugen.
3. Die Regeln (Lieferantenliste, Limits, Warengruppen) als Vollmacht hinterlegen, freigegeben durch die Einkaufsleitung.
4. Im Agenten vor dem Absenden einer Bestellung einen Prüfaufruf an die MolTrust-Schnittstelle einbauen (Bibliotheken für Node.js und Python verfügbar).
5. Die Prüfprotokolle an das bestehende Logging oder SIEM anbinden.
6. Das ERP-System (z. B. SAP Business One, proALPHA) bleibt unverändert; der Agent bestellt über die bestehenden Wege.

Allgemeiner Integrationsablauf

- **Aufwand:** Die Einbindung von MolTrust dauert wenige Minuten: API-Schlüssel holen, Agent registrieren, Prüfaufruf vor die Aktion setzen. Schritt für Schritt im Quickstart auf moltrust.ch/developers.
- **Bestehende Systeme:** ERP, Shop, Buchhaltung bleiben unverändert; MolTrust sitzt als Prüfschritt vor der Aktion des Agenten.
- **Zuständigkeit:** Fachabteilung legt die Regeln fest, IT baut den Prüfaufruf ein.
- **Datenschutz:** Geprüft werden Befugnisse und Aktion; Geschäftsdaten bleiben im Unternehmen.
- **Grundsatz:** Was nicht ausdrücklich erlaubt ist, wird abgelehnt.

Begriffe: DID (Decentralized Identifier, eine fälschungssichere digitale Identität für einen Agenten). VC (Verifiable Credential, ein digital signierter Nachweis, z. B. über eine Befugnis). AAE (Agent Authorization Envelope, das Vollmachts-Format von MolTrust, das festlegt, was ein Agent darf). SIEM (Security Information and Event Management, zentrale Sicherheits-Protokollauswertung).

Kontakt
hello@moltrust.ch · https://moltrust.ch/use-cases/einkauf/