Lansweeper: IT-Inventar neu denken und meistern

Category: Online-Marketing
geschrieben von Tobias Hager | 5. Februar 2026



Lansweeper: IT-Inventar neu denken und meistern

Dein Unternehmen brennt nicht – aber deine IT-Infrastruktur ist ein Pulverfass. Du weißt nur noch nicht, wo genau der Zünder liegt. Du hast keine Ahnung, welche Geräte wirklich im Netzwerk hängen, welche Software-Versionen auf den Rechnern gammeln und wo das nächste Sicherheitsleck lauert? Willkommen in der Realität von 90 % der Unternehmen. Und genau hier setzt Lansweeper an – nicht als fancy Tool, sondern als radikale Inventarlösung für IT-Profis, die keine Lust auf Überraschungen mehr haben.

- Was Lansweeper ist – und warum es dein IT-Inventar auf links dreht
- Warum klassische Asset-Management-Methoden einfach nicht mehr reichen
- Wie Lansweeper deine gesamte IT sichtbar macht – automatisch und präzise
- Die technischen Features von Lansweeper im Detail: Scans, Agenten, APIs

- Datensicherheit, DSGVO und Compliance-Fragen rund um Lansweeper
- Best Practices für den Einsatz in komplexen IT-Landschaften
- Wie Lansweeper mit anderen Tools wie SCCM, Intune oder ServiceNow zusammenspielt
- Typische Fehler bei der Einführung – und wie du sie vermeidest
- Ein Ausblick auf die Zukunft von IT-Asset-Management mit Lansweeper

Lansweeper erklärt: Was kann das Tool wirklich?

Lansweeper ist kein weiteres IT-Tool, das hübsche Dashboards und bunte Icons liefert, aber am Ende nichts tut. Es ist ein knallhartes IT-Asset-Management-System (ITAM), das entwickelt wurde, um dir volle Transparenz über deine gesamte IT-Infrastruktur zu geben – und zwar ohne, dass du jedes Gerät manuell anfassen musst. Klingt nach Zauberei? Ist aber pure Technik.

Im Kern ist Lansweeper ein automatisiertes Discovery-Tool, das Hard- und Software-Ressourcen in deinem Netzwerk identifiziert, katalogisiert und überwacht. Das bedeutet konkret: Jeder Client, jeder Server, jedes IoT-Gerät und jede Software-Instanz, die sich in deinem Netzwerk tummelt – Lansweeper findet sie. Und das nicht nur oberflächlich, sondern mit tiefen Scanverfahren, die selbst versteckte Assets aus der Versenkung holen.

Das Tool arbeitet agentenlos oder agentenbasiert – je nach Infrastruktur und Sicherheitsanforderung. Es nutzt Protokolle wie WMI, SNMP, SSH, HTTP(S), WinRM oder auch Remote Registry, um detaillierte Informationen aus Systemen zu ziehen. Du willst wissen, welche Windows-Version auf welchem Gerät läuft, ob ein BIOS-Update fehlt oder ob ein Gerät seit sechs Monaten offline ist? Lansweeper hat die Antwort. In Echtzeit. Ohne manuelle Eingriffe.

Und das Beste: Lansweeper ist skalierbar. Egal ob du fünfzig Devices oder fünfzigtausend verwalten willst – das Tool wächst mit dir. Es integriert sich nahtlos in bestehende Systeme und bietet APIs sowie Konnektoren zu gängigen ITSM- und CMDB-Lösungen. Das macht es zum strategischen Backbone für modernes IT-Management.

Warum klassisches Asset-Management tot ist – und Lansweeper die Antwort liefert

Die Zeiten, in denen IT-Administratoren mit Excel-Listen gearbeitet haben, sind offiziell vorbei – oder sollten es zumindest sein. Denn in einer Welt, in der hybride Arbeitsmodelle, BYOD (Bring Your Own Device), Cloud-Services und Shadow-IT die Norm sind, ist manuelles Asset-Tracking schlichtweg absurd. Es ist fehleranfällig, aufwendig und gefährlich. Und es kostet dich nicht nur

Nerven, sondern auch Compliance, Sicherheit und Geld.

Das größte Problem klassischer Systeme: Sie sind statisch. Einmal erfasst, veralten die Daten innerhalb von Tagen – oder Stunden. Updates müssen manuell eingepflegt werden, Gerätewechsel werden nicht automatisch erkannt, und Software-Änderungen bleiben oft unbemerkt. Das Ergebnis? Ein IT-Inventar, das bestenfalls eine Momentaufnahme ist – und schlimmstenfalls eine Illusion.

Hinzu kommt die Intransparenz. In vielen Unternehmen weiß niemand genau, welche Geräte existieren, wie sie konfiguriert sind oder wem sie gehören. Und das öffnet Tür und Tor für Sicherheitsprobleme: veraltete Betriebssysteme, fehlende Patches, nicht autorisierte Geräte. Die Angriffsfläche wächst – und du hast keinen Überblick.

Lansweeper löst dieses Problem radikal. Das Tool scannt kontinuierlich deine gesamte Infrastruktur und aktualisiert die Datenbank in Echtzeit. Neue Geräte? Sofort erkannt. Softwareänderungen? Direkt dokumentiert. Lizenzverletzungen? Automatisch markiert. So entsteht ein lebendiges, dynamisches IT-Inventar, das nicht nur dokumentiert, sondern analysiert, warnt und steuert.

Technischer Deep Dive: Wie Lansweeper wirklich funktioniert

Technisch gesehen ist Lansweeper ein hybrides Scan-Tool, das sowohl agentenlose als auch agentenbasierte Scans durchführen kann. Der Hauptvorteil dabei: Flexibilität. Du kannst je nach Use Case entscheiden, ob du auf Remote-Zugriff über WMI, SNMP, SSH etc. setzt – oder mit einem lokal installierten Agenten arbeitest, der Daten auch außerhalb des Netzwerks (z. B. bei mobilen Geräten) sammelt.

Die Hauptkomponenten im Überblick:

- Scanning Engine: Führt Netzwerk-Scans durch, erkennt Geräte und sammelt Systeminformationen.
- Asset-Datenbank: Zentrale SQL-Datenbank, in der alle gesammelten Informationen gespeichert und korreliert werden.
- Web Console: Administrationsoberfläche für die Analyse, Berichterstellung, Konfiguration und Automatisierung.

Ein technisches Highlight ist die Verwendung von Credential Sets. Damit kannst du unterschiedliche Zugriffsrechte für verschiedene Gerätekategorien hinterlegen – z. B. Windows-Domänenzugänge, SSH-Keys für Linux-Systeme oder SNMP-Strings für Netzwerktechnik. All das erfolgt verschlüsselt und zentral gesteuert.

Besonders spannend: Die Integration von benutzerdefinierten Feldern, Tags und Automatisierungsregeln. So kannst du Assets nach Belieben klassifizieren,

Warnungen definieren (z. B. bei veralteten Firmware-Versionen) und automatisiert Tickets in dein ITSM-System pushen. Lansweeper wird damit nicht nur zum Inventar-Tool, sondern zum aktiven Steuerinstrument deiner IT.

Datenschutz, DSGVO und Lansweeper: Was du wissen musst

Kaum ein IT-Tool kommt heute ohne Datenschutzdebatte aus – und Lansweeper ist da keine Ausnahme. Doch die gute Nachricht: Das Tool ist von Grund auf so konzipiert, dass es DSGVO-konform betrieben werden kann. Aber – und das ist entscheidend – es liegt an dir, es korrekt zu konfigurieren.

Grundsätzlich speichert Lansweeper nur technische Informationen über Geräte, Software, Netzwerkkonfigurationen etc. Personenbezogene Daten werden nicht automatisch gesammelt – es sei denn, du konfigurierst es so. Wenn du z. B. Usernamen, E-Mail-Adressen oder persönliche Identifikatoren erfasst, musst du sicherstellen, dass diese Daten rechtlich abgesichert sind.

Das bedeutet konkret:

- Datenschutzfolgeabschätzung (DSFA) durchführen
- Verzeichnis von Verarbeitungstätigkeiten aktualisieren
- Zugriffsrechte im Tool granular verteilen
- Datenbankverschlüsselung aktivieren
- Backups DSGVO-konform speichern

Wichtig: Lansweeper selbst ist on-premises oder als Cloud-Version verfügbar. Bei der Cloud-Variante solltest du prüfen, wo die Daten gespeichert werden (z. B. in EU-Rechenzentren) und ob ein AV-Vertrag besteht. Die lokale Variante gibt dir volle Kontrolle über alle Daten – ist aber natürlich wartungsintensiver.

Best Practices für Lansweeper in der Praxis

Ein Tool ist nur so gut wie seine Implementierung. Und auch Lansweeper kann zur Datenhölle werden, wenn du es ohne Plan einführst. Deshalb hier eine Liste bewährter Best Practices, wie du das Maximum aus dem Tool herausholst:

- Vor dem Rollout: Netzwerkstruktur analysieren, Subnetze planen, Credential Sets vorbereiten
- Scan-Scheduling: Regelmäßige, differenzierte Scans einrichten – z. B. tägliche Scans für kritische Systeme, wöchentliche für Peripherie
- Asset-Tags & Kategorien: Geräte nach Funktion, Standort oder Abteilung taggen für bessere Filterbarkeit

- Berichte automatisieren: Regelmäßige Reports per Mail versenden – z. B. über neue Geräte, auslaufende Softwarelizenzen oder Offline-Systeme
- Integrationen nutzen: Lansweeper mit ITSM-Tools wie ServiceNow, Freshservice oder Jira verbinden
- Regelmäßige Audits: Datenqualität prüfen, Dubletten bereinigen, ungenutzte Assets archivieren

Richtig umgesetzt, wird Lansweeper zur zentralen Quelle der Wahrheit über deine IT – und damit zur Grundlage für jede fundierte Entscheidung im IT-Betrieb.

Fazit: Lansweeper ist kein Spielzeug – es ist Pflichtwerkzeug

Wer heute IT betreibt, ohne ein professionelles, automatisiertes Inventarsystem wie Lansweeper, handelt fahrlässig. Punkt. Die Komplexität moderner IT-Infrastrukturen lässt sich nicht mehr mit manuellen Listen, Bauchgefühl oder veralteten Tools managen. Die Risiken – von Compliance-Verstößen über Sicherheitslücken bis hin zu Audit-Desastern – sind zu groß.

Lansweeper ist kein nettes Add-on, sondern ein strategischer Gamechanger. Es liefert dir nicht nur Daten, es liefert dir Kontrolle. Und Kontrolle ist in der IT das, was Sichtbarkeit im Marketing oder Liquidität in der Buchhaltung ist: existenziell. Wenn du deine IT wirklich verstehen, sichern und optimieren willst, brauchst du Lansweeper. Alles andere ist blindes Vertrauen – und das hat in der IT noch nie funktioniert.