

sayTRUST UZE

LÖSUNG UND ARCHITEKTUR

Automatisierte VDI und PAW

Virtuelle Arbeitsplätze und privilegierter Zugriff

Der geschützte digitale Arbeitsplatz

- Virtuelle Arbeitsplätze
- Privilegierte Administration
- Automatisierte Bereitstellung

Inhalt

Executive Summary

Von der VDI zur Privileged Access Workstation

Abkapselung durch Post Zero Trust

Automatisierung vom Profil bis zur Freigabe

Software und Arbeitsplatz im Lebenszyklus

Einsatz in sensiblen Arbeitsumgebungen

Umsetzung und überprüfbarer Nutzen

Fazit

Executive Summary

Die Sicherheit eines virtuellen Arbeitsplatzes beruht auf einer streng abgestimmten Konfiguration, kontrollierter Softwarebereitstellung und klar geregelten Anwendungszugriffen. Golden Image, Ressourcenprofil, Anwendungen, Berechtigungen und zulässige Kommunikationsbeziehungen werden festgelegt und überprüfbar dokumentiert. Die VDI-Plattform stellt die virtuelle Arbeitsplatzinstanz bereit, Matrix42 verteilt die freigegebenen Softwarepakete und sayTRUST UZE beschränkt den Zugriff auf ausdrücklich autorisierte Anwendungen und Dienste.

Für Facharbeit, Entwicklung und privilegierte Administration werden getrennte Profile verwendet. Eine PAW ist ein dedizierter, gehärteter Arbeitsplatz für privilegierte Aufgaben; sie entsteht nicht allein durch Virtualisierung. Sowohl der Zugang zur VDI als auch die Kommunikation aus der VDI zu ihren Zielsystemen benötigen eigene Freigaben.

Die Automatisierung umfasst Erstbereitstellung, Domänen- und UEM-Registrierung, Paketinstallation, Baseline-Prüfung sowie die Änderung und Rückgabe. Vorbereitete Instanzen können nach der Zugriffsprüfung zugewiesen werden. Bei neu erzeugten Instanzen wird die produktive Nutzung erst nach Umsetzung der verpflichtenden Baseline freigegeben. Das reduziert manuelle Einzelkonfigurationen und macht den Arbeitsplatz reproduzierbar.

Das gemeinsame Betriebsmodell umfasst interne und mobile Arbeitsplätze, mehrere Standorte sowie getrennte Mandanten. Eine resiliente HCI-Plattform, unabhängige Sicherheitsstände und bei Bedarf LiveSync unterstützen die Verfügbarkeit der Arbeitsumgebungen und deren Wiederherstellung im Störfall. Der Nutzen lässt sich anhand konkreter Kriterien bewerten: der Bereitstellungszeit, der Einhaltung freigegebener Konfigurationen, der Wirksamkeit und Geschwindigkeit des Rechteentzugs sowie der Ergebnisse regelmäßig getesteter Wiederanläufe.

Automatisierte VDI und PAW

Geprüfte Identität, autorisierter User, freigegebene Software und Umgebung und kontrollierter Zugriff

Dieses Whitepaper beschreibt die automatisierte Bereitstellung geschützter virtueller Arbeitsplätze und dedizierter Privileged Access Workstations. Es verbindet sayFUSE HCI, sayTRUST UZE und Matrix42 UEM/ Empirum zu einem abgestimmten Prozess vom definierten Arbeitsplatzprofil bis zum kontrollierten Neuaufbau.

1. Von der VDI zur Privileged Access Workstation

Eine VDI beschreibt zunächst die virtuelle Bereitstellung eines Desktops. Eine PAW beschreibt dessen Sicherheitszweck: einen dedizierten, gehärteten Arbeitsplatz für privilegierte Aufgaben. Die Bezeichnung PAW ist deshalb an wirksam umgesetzte Kontrollen gebunden und ergibt sich nicht allein aus der Virtualisierung.

Arbeitsplatzprofil	Aufgabe und Abgrenzung
Geschützter Facharbeitsplatz	Vertrauliche Vorgangsbearbeitung und freigegebene Kommunikation. Keine pauschalen Administrationsrechte.
Privileged Access Workstation	Dedizierte Administration definierter Systeme. Getrennte privilegierte Identität, eng begrenzte Werkzeuge und Zielzugriffe.
Geschützter Entwicklungsarbeitsplatz	Freigegebene Entwicklungsumgebungen, Repositories und Build-Dienste. Produktive Administration erfolgt über ein separates PAW-Profil.

Was eine virtuelle PAW voraussetzt

Zum PAW-Profil gehören ein gehärtetes Betriebssystem, eine kontrollierte Anwendungsauswahl, getrennte administrative Konten und die Beschränkung auf freigegebene Zielsysteme. Allgemeines Surfen und gewöhnliche E-Mail-Nutzung werden von der privilegierten Umgebung getrennt. Zusätzliche Rechte werden nur für den erforderlichen Zweck und Zeitraum vergeben. Wo vorgesehen, ergänzt eine PAM-Lösung die Rechtevergabe und Sitzungssteuerung.

Das zugreifende Gerät ist Teil der Schutzkette. Ein kompromittierter lokaler Rechner kann Eingaben oder eine bereits autorisierte Sitzung gefährden. Eine virtuelle PAW und ein geschützter Transport neutralisieren dieses Risiko nicht automatisch. Für die privilegierte Nutzung sind deshalb entsprechend gehärtete, verwaltete Zugriffsgeräte und überprüfbare Zulassungsregeln erforderlich. [2]

Der Steuerungsebene kommt besonderer Schutz zu

Wer Golden Images, Hypervisoren, VDI-Broker, Verteilungspakete oder Identitäten verändern kann, beeinflusst die Sicherheitsarbeitsplätze. Diese Verwaltungszugriffe werden getrennt, minimal berechtigt und über eigene privilegierte Zugangswege ausgeführt. Die Berechtigung zum Arbeiten in einer VDI umfasst nicht die Berechtigung, ihre Plattform oder ihre Baseline zu administrieren.

Sicherheitsprofil und Aufgabenprofil müssen zusammenpassen

Ein Entwickler benötigt andere Werkzeuge als ein Administrator oder ein Sachbearbeiter im Ministerium. Die gemeinsame Automatisierung liefert daher mehrere freigegebene Profile. Besonders sensible Entwicklungsaktionen, der Produktionszugriff oder die Verwaltung von Signierschlüsseln, werden organisatorisch und technisch von alltäglichen Entwicklungsarbeiten getrennt.

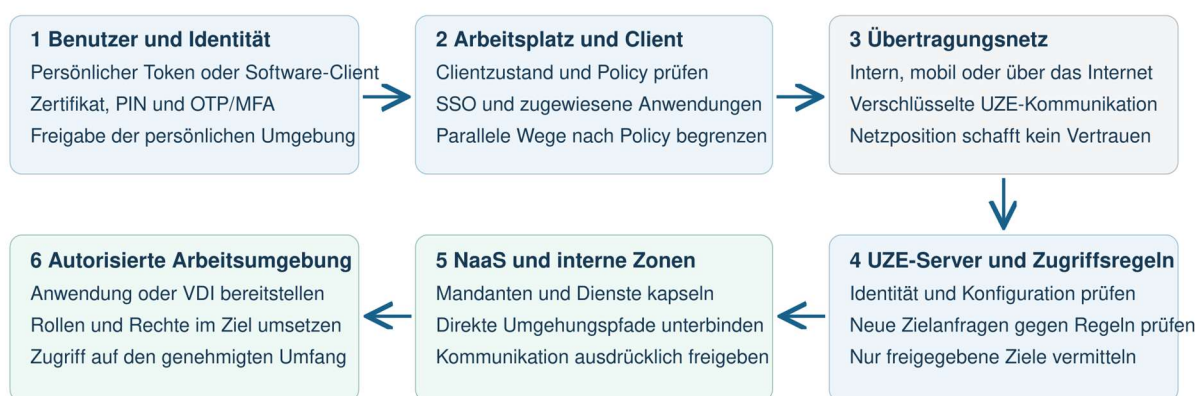
2. Abkapselung durch Post Zero Trust

Post Zero Trust bezeichnet hier das sayTEC-Architekturmodell zur gezielten Isolation autorisierter Anwendungs- und Kommunikationsbeziehungen. Es ergänzt Zero-Trust-Grundsätze. Die Sicherheitsentscheidung fällt vor der Freigabe des Kommunikationswegs.

Die Zugriffskette

Im beschriebenen UZE-Modell wird nach erfolgreicher Identitäts-, Client- und Berechtigungsprüfung die geschützte Client-Umgebung freigegeben. Je nach Variante erfolgt dies hardware- oder softwarebasiert. Der geschützte temporäre Laufzeitkontext dient der sitzungsbezogenen Verarbeitung sicherheitsrelevanter Informationen. Die Domänen- beziehungsweise VDI-Anmeldung folgt innerhalb des zugelassenen Zugangswegs; sie ersetzt die vorgelagerte UZE-Prüfung nicht.

Die kontrollierte Strecke vom Benutzer zur Anwendung



Eine Sicherheitslogik für interne und externe Arbeitsplätze

Kein allgemeiner Zugang zu geschützten Netzen – nur ausdrücklich freigegebene Beziehungen.

Abb. 1: Die UZE-Strecke verbindet Benutzer, zugelassenes Endgerät, Übertragungsnetz und autorisierten Zielzugriff. Die VDI erhält ein eigenes Aufgaben- und Kommunikationsprofil.

Vom lokalen Gerät bis zum Zielsystem

Die erste Grenze liegt zwischen Zugriffsgerät und VDI-Dienst. Nur die freigegebene Beziehung wird zugelassen; ein allgemeiner Netzwerkzugang des lokalen Geräts ist nicht Bestandteil des Modells. Die zweite Grenze liegt zwischen dem virtuellen Arbeitsplatz und seinen Zielressourcen. Auch dort sind Ziele, Protokolle und erforderliche Abhängigkeiten ausdrücklich festzulegen.

Die zweite Grenze entsteht nicht automatisch durch den geschützten VDI-Zugang. Sie wird durch die dafür ausgelegte UZE-Integration und ergänzende Kontrollen wie Host-Firewalls, Netzwerkregeln und Zielsystemberechtigungen umgesetzt. Verbindungen zu Identitätsdiensten, UEM, Monitoring, Updates und anderen Betriebsdiensten müssen dabei gezielt berücksichtigt werden.

Datenübergänge werden ausdrücklich geregelt

Zwischenablage, Laufwerks- und USB-Umleitung, Druck, Dateiübertragung sowie parallele Kommunikationswege werden je Profil erlaubt, begrenzt oder gesperrt. Die Durchsetzung erfolgt durch die zuständigen VDI-, Endgeräte- und Zugriffskontrollen. Eine pauschale Produktzusage für sämtliche Kanäle ist daraus nicht abzuleiten.

„Abgekapselt“ bedeutet in dieser Architektur, dass außerhalb der definierten und geprüften Beziehungen keine freigegebenen Kommunikationspfade bestehen. Der Begriff bezeichnet weder eine physische Netztrennung

noch Unangreifbarkeit. Die tatsächliche Isolation wird durch Positiv- und Negativtests der jeweiligen Implementierung nachgewiesen.

Autorisierte Beziehungen können je nach Einsatzfall Programme, Dienste, Maschinenzugriffe sowie Sprach- und Videokommunikation zulassen. Solche Funktionen werden nur in den dafür freigegebenen Profilen bereitgestellt. Eine administrative PAW erhält deshalb nicht automatisch die Kommunikationsfunktionen eines allgemeinen Facharbeitsplatzes.

3. Automatisierung vom Profil bis zur Freigabe

Der Bereitstellungsprozess setzt eine zuvor freigegebene Konfiguration um. Die Automatisierung ersetzt dabei keine fachliche oder sicherheitstechnische Entscheidung, sondern führt sie nachvollziehbar aus.

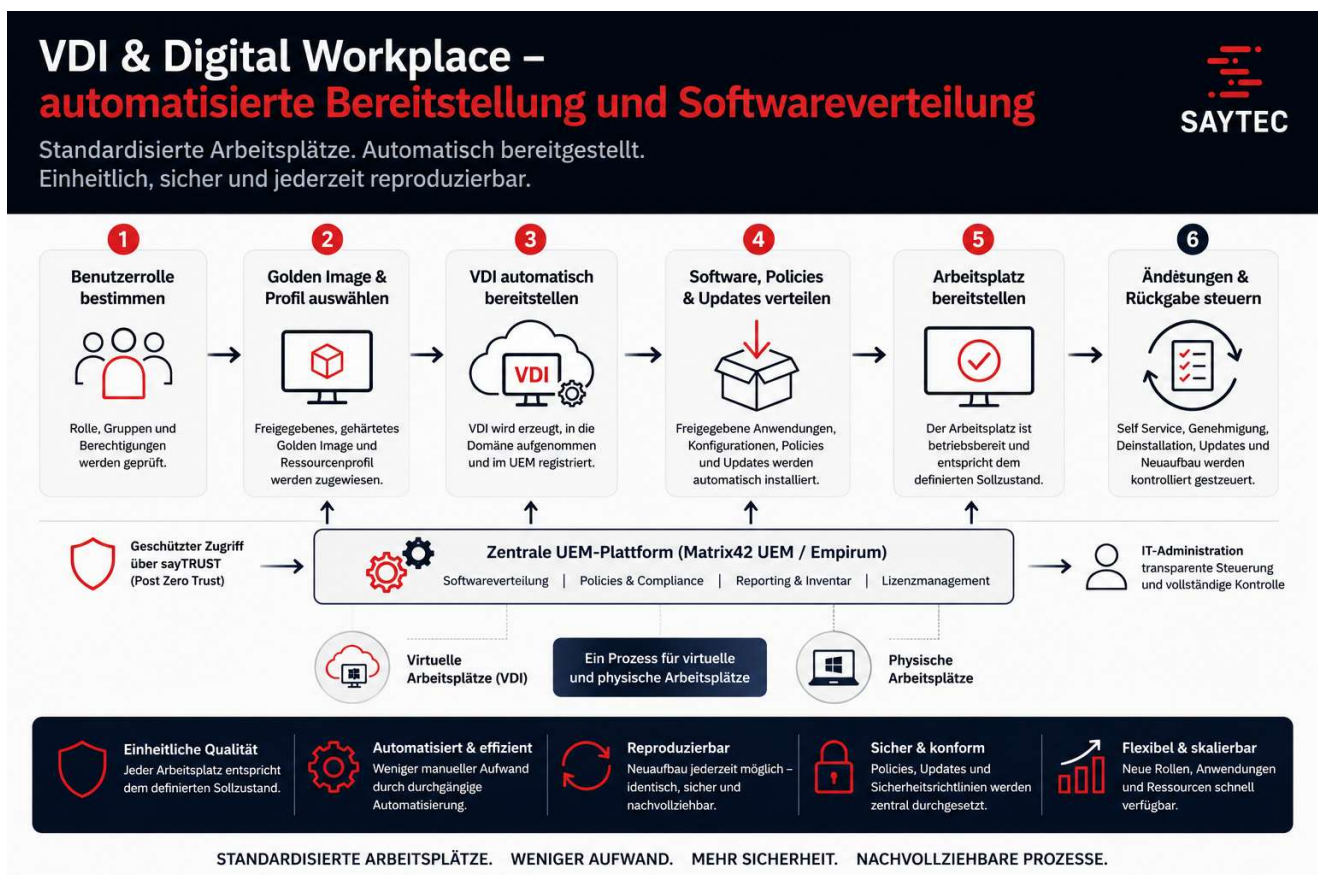


Abb. 2: Automatisierte VDI-Bereitstellung, Softwareverteilung und kontrollierter Lebenszyklus. UZE, VDI-Plattform und UEM erfüllen unterschiedliche Aufgaben innerhalb desselben Prozesses.

Baustein	Verantwortung
Betreiber und Freigabeverantwortliche	Definieren von Rollen, Schutzbedarf, Profile, Zielsysteme, Pakete und Genehmigungswege.
sayTRUST UZE	Prüft den konfigurierten Zugang und vermittelt freigegebene Kommunikationsbeziehungen.
VDI-Plattform auf sayFUSE HCI	Erzeugt oder weist Instanzen zu und stellt Ressourcen sowie Netzwerkzonen bereit.
Domäne und Identitätsdienste	Authentifizieren die Domänenidentität und liefern Rollen und Gruppenzugehörigkeiten.
Matrix42 UEM / Empirum	Registriert Endpoints, verteilt freigegebene Pakete und meldet Ausführungsstatus zurück.
Service Catalog und integrierte Orchestrierung	Steuern Genehmigung, technische Zuordnung, Freigabezustände und Fehlerbehandlung.

Schritt 1 - Rollen und Schutzbedarf festlegen

Der Betreiber definiert Nutzergruppen, Aufgaben, Verantwortliche und Zielsysteme. Daraus entstehen getrennte Fach-, Entwicklungs- und PAW-Profile mit ihren Berechtigungen und Kommunikationsregeln. Auch die Anforderungen an das zugreifende Gerät werden je Profil festgelegt.

Schritt 2 – Golden Image und Baseline freigeben

Das Golden Image wird in einer getrennten Build- und Testumgebung erstellt, gehärtet und versioniert. Betriebssystem, benötigte Agenten und Basiskomponenten werden geprüft. CPU, RAM, Storage, Netzwerkzone und Persistenzmodell werden im VDI-Profil festgelegt. Verpflichtende Pakete und Konfigurationen vervollständigen die Baseline. Golden Image und Baseline werden nach erfolgreicher Prüfung freigegeben.

Schritt 3 – Instanz erzeugen und eindeutig registrieren

Die VDI-Orchestrierung erstellt eine neue Instanz oder weist eine vorbereitete Instanz zu. Bei der Erstbereitstellung erfolgen die vorgesehene Domänenintegration sowie die eindeutige Geräte- und UEM-Agentenregistrierung. Bestehende Instanzen werden bei einer normalen Anmeldung nicht erneut integriert oder registriert.

Auch geklonte Instanzen benötigen eindeutige Geräte- und Agentenidentitäten. Der Integrationsprozess verhindert doppelte Zuordnungen und stellt sicher, dass veraltete Computerobjekte kontrolliert bereinigt werden.

Schritt 4 – Softwarezustand automatisiert herstellen

Matrix42 UEM/Empirum wertet die freigegebenen Zuordnungen aus und verteilt Pakete, Konfigurationen und Updates. Abhängigkeiten, Neustarts und Installationsreihenfolgen werden im Paket- und Betriebsmodell festgelegt. Fehler werden zurückgemeldet. Solange verpflichtende Komponenten nicht erfolgreich installiert oder konfiguriert sind, bleibt die Nutzungsfreigabe gesperrt.

Schritt 5 - Baseline prüfen und Nutzung zulassen

Ein erfolgreicher Installationsauftrag allein ist noch keine Betriebsfreigabe. Die integrierte Orchestrierung muss den Zustand anhand definierter Kriterien prüfen: erforderliche Pakete, aktiver Schutz, richtige Identität und wirksame Kommunikationsregeln. Nur eine freigegebene Instanz wird dem Nutzer für die vorgesehene Aufgabe zugänglich gemacht.

Schritt 6 - Anmeldung und laufenden Zustand steuern

Der Nutzer durchläuft die UZE-Zugriffsprüfung und meldet sich am freigegebenen VDI-Dienst an. Vorbereitete Desktops können sofort zugewiesen werden; bei bedarfsgesteuerter Erzeugung wartet die Nutzungsfreigabe auf die Baseline. Im Betrieb führen Rollenänderungen und Sicherheitsabweichungen zu den definierten Einschränkungen, Korrekturen oder Sperren.

Erstbereitstellung und normale Anmeldung

Bei einem neuen Arbeitsplatz wird nach der Zugriffs- und Rollenprüfung die passende Instanz erstellt oder aus einem vorbereiteten Pool zugewiesen. Die benötigte Infrastruktur- und Domänenintegration sowie Software-Baseline werden umgesetzt. Bei einer bestehenden, konformen Instanz genügt der vorgesehene Zugriffs- und Anmeldeprozess; nur anstehende Änderungen werden entsprechend den Betriebsregeln verarbeitet. So bleibt der Ablauf nachvollziehbar, ohne bei jedem Login unnötige Installationsschritte zu wiederholen.

4. Software und Arbeitsplatz im Lebenszyklus

Zusatzsoftware bleibt eine kontrollierte Änderung

Zusätzliche Anwendungen werden aus einem freigegebenen Servicekatalog beantragt. Fachliche Zuständigkeit, Sicherheitsbewertung und Lizenzbedarf bestimmen den Genehmigungsweg. Für PAWs ist ein besonders eng gefasster Katalog vorgesehen. Die Freigabe einer Anwendung für einen Facharbeitsplatz gilt nicht automatisch für ein privilegiertes Profil.

Nach der Genehmigung wird über den integrierten Service-Management-Prozess die technische Zuordnung erstellt. Empirum übernimmt die Softwareverteilung; Statusmeldungen und Fehler werden an den Workflow zurückgemeldet. Voraussetzung dafür ist, dass die benötigten Matrix42-Komponenten, Connectoren und Workflows eingerichtet sind. [3]

Änderung	Freigabe und Abschluss
Standardsoftware	Freigegebener Katalog; automatische oder fachliche Freigabe entsprechend der Rolle.
Lizenzpflichtige Anwendung	Zusätzliche Prüfung von Lizenzbestand und Kostenstelle.
Sicherheitskritische oder privilegierte Werkzeuge	Zusätzliche Sicherheitsfreigabe, enger Zielumfang und gegebenenfalls zeitliche Befristung.
Rückgabe	Zuordnung entziehen, Deinstallation auslösen und prüfen, Lizenz entsprechend der hinterlegten Logik zurückführen.

Rückgabe wird technisch abgeschlossen

Eine Rückgabe muss einen geeigneten Deinstallationsauftrag auslösen und dessen Ergebnis prüfen. Das bloße Entfernen einer Zuordnung belegt noch keine Entfernung der Software. Matrix42 beschreibt für die Servicerückgabe den Empirum-Befehl „Uninstall“. Lizenzrückführung und Abschlussstatus folgen der hinterlegten Logik und dem nachgewiesenen Ergebnis. [3]

Updates und Neuaufbau bleiben reproduzierbar

Neue Images und Paketversionen durchlaufen Tests und eine Pilotierung, bevor sie produktiv verteilt werden. Für Fehlerfälle werden Verfahren zum Zurückrollen, zur Sperrung oder zum Neuaufbau auf Basis einer freigegebenen Version festgelegt. Paketquellen und die Berechtigungen zu ihrer Änderung sind Teil der Sicherheitsarchitektur.

Bei nichtpersistenten VDIs müssen dauerhafte Änderungen im Image oder im wiederherstellbaren Sollzustand abgebildet sein. Nutzerprofile und genehmigte Softwareberechtigungen werden unabhängig von kurzlebigen Instanzen verwaltet. Auch bei persistenten VDIs müssen Abweichungen vom Sollzustand erkannt und korrigiert werden. Verwaiste Instanzen, Geräteobjekte und nicht mehr benötigte Berechtigungen werden kontrolliert bereinigt.

Ein fehlgeschlagenes Pflichtpaket oder eine unvollständige Baseline wird als Fehlerzustand sichtbar. Wiederholungslogik, Korrektur und Eskalation sind je Paket festgelegt. Bis zur erfolgreichen Prüfung bleibt die produktive Nutzungsfreigabe gesperrt; der Installationsstatus wird nicht mit dem fachlichen Abschluss des Arbeitsplatzes verwechselt.

Kommunikationsfreigaben ändern sich mit der Aufgabe

Ein Rollenwechsel kann Anwendungen und Zielzugriffe entziehen. Der Entzug muss deshalb Softwarezuordnungen, Identitätsrechte, UZE-Policies und gegebenenfalls aktive Sitzungen berücksichtigen. Eine zeitlich befristete Freigabe benötigt einen definierten Ablauf und eine überprüfbare Beendigung.

Reproduzierbarkeit ist noch keine vollständige Wiederherstellung

Ein neu erzeugbarer Desktop ersetzt kein Backup seiner benötigten Daten, Profile, Konfigurationen und abhängigen Dienste. Der Betreiber legt Wiederanlaufreihenfolge, RTO und RPO fest und testet die Wiederherstellung. Eine resiliente Betriebsplattform, beispielsweise sayFUSE HCI bei entsprechender Auslegung, kann die Verfügbarkeit ergänzen; Backup und Disaster Recovery sichern weitere Fehlerfälle ab.

Einordnung in die ganzheitliche Infrastruktur

sayFUSE HCI trägt die virtuellen Arbeitsplätze und ihre abhängigen Dienste. NaaS trennt Fachbereiche, Entwicklung, PAW, Management und Sicherung. sayTRUST UZE begrenzt die freigegebenen Zugriffswege. sayFUSE Backup hält unabhängige Generationen für Profile, Daten und relevante Plattformkonfigurationen vor. LiveSync kann priorisierte Dienste auf einer zweiten Betriebsumgebung fortführen, während die ursprüngliche Plattform repariert wird. Nach erfolgreicher Prüfung erfolgt die kontrollierte Rücksynchronisation und Rückumschaltung.

5. Einsatz in sensiblen Arbeitsbereichen

Botschaften und Auslandsvertretungen

Ein zentral gesteuertes Facharbeitsplatzprofil kann den Zugriff auf freigegebene Vorgänge und Kommunikationsdienste über Standorte hinweg vereinheitlichen. Datenübergänge und lokale Umleitungen werden dem Schutzbedarf entsprechend eingeschränkt. Technische Administratoren erhalten davon getrennte PAW-Profile. Standortanbindung, Ausfallszenarien sowie Vorgaben zu Datenhaltung und Betrieb bestimmen die konkrete Auslegung.

Ministerien und öffentliche Einrichtungen

Für unterschiedliche Fachbereiche lassen sich definierte Arbeitsplatzprofile mit zentralen Freigaben und nachvollziehbarer Softwareverteilung bereitstellen. Privilegierte Zugriffe auf Identitätsdienste, Fachverfahren oder die Infrastruktur erfolgen über dedizierte Verwaltungsprofile. Eine vertrauliche Fachaufgabe allein begründet keine zusätzlichen Administrationsrechte.

Administration und externe Spezialisten

Eine PAW stellt die für den jeweiligen Auftrag freigegebenen Werkzeuge und Zielbeziehungen bereit. Zeitlich begrenzte Berechtigungen, getrennte administrative Identitäten und die nachvollziehbare Beendigung des Auftrags begrenzen den Zugriff. Externe Spezialisten benötigen ebenfalls ein zugelassenes Zugriffsgerät; eine externe Rolle rechtfertigt keinen allgemeinen Netzzugang.

Entwicklung und technische Projektarbeit

Entwicklungsprofile enthalten geprüfte Werkzeuge und definierte Beziehungen zu Repositories, Artefaktquellen, Build-Diensten und Testsystemen. Externe Pakete und Internetabhängigkeiten werden über kontrollierte Quellen und Freigabewege eingebunden. So lässt sich ein projektbezogener Entwicklungsarbeitsplatz reproduzierbar erzeugen, ohne jedem Entwickler pauschale Infrastrukturrechte zu geben.

Produktive Administration, Deployment-Freigaben oder Schlüsselverwaltung werden separat berechtigt und bei Bedarf über eine eigene PAW ausgeführt. Quellcode und Entwicklungswerkzeuge gehören nicht automatisch in dieselbe Vertrauenszone wie produktive Administrationsidentitäten.

Besondere Schutzklassen erfordern eigene Freigaben

Die beschriebenen Profile sind ein Architekturansatz für sensible Tätigkeiten. Ihre Eignung für konkrete Geheimhaltungsgrade, behördliche Zulassungen oder besondere Kommunikationsanforderungen muss gesondert festgestellt werden. Weder eine VDI noch die Bezeichnung PAW ersetzt die erforderliche Prüfung und Freigabe des Gesamtsystems.

6. Umsetzung und überprüfbarer Nutzen

Der Einstieg erfolgt über ein begrenztes, repräsentatives Profil mit klaren Zielsystemen. Nach erfolgreicher Abnahme können weitere Rollen und Standorte mit denselben freigegebenen Bausteinen bedient werden.

Verantwortlichkeiten festlegen

Der Betreiber verantwortet Schutzbedarf, Rollen und Freigaben. Die VDI-Plattform verantwortet Instanzen und Ressourcen; Matrix42 die eingerichteten Endpoint- und Softwareprozesse. sayTRUST UZE steuert die dafür konfigurierte Zugangsebene. Die Integration muss Statusübergänge, Sperren und Fehlerbehandlung systemübergreifend umsetzen.

Die Abnahme muss die Schutzwirkung nachweisen

Zugriff: Unberechtigte Identitäten und nicht zugelassene Geräte werden abgewiesen; erlaubte Nutzer erreichen ausschließlich die freigegebenen Dienste.

Isolation: Nicht freigegebene Ziele sind sowohl vom lokalen Gerät als auch aus der VDI nicht erreichbar; erlaubte Betriebsabhängigkeiten bleiben funktionsfähig.

Arbeitsplatz: Eine unvollständige Baseline verhindert die Nutzungsfreigabe. Datenumleitungen und getrennte Administrationsrollen wirken wie vorgesehen.

Lebenszyklus: Installation, Entzug, Rechteablauf und Neuaufbau werden praktisch geprüft; Ausfall- und Wiederherstellungstests belegen die festgelegten Betriebsziele.

Erfolg messbar machen

Geeignete Kennzahlen sind die Zeit bis zur Nutzungsfreigabe, der Anteil vollständig konformer Arbeitsplätze, die Anzahl fehlgeschlagener Bereitstellungen, die Zeit bis zum wirksamen Rechteentzug und die gemessene Wiederherstellungszeit. Sie zeigen, ob Automatisierung und Sicherheitskontrollen im Betrieb wirksam zusammenspielen.

Praxisablauf für einen neuen Benutzer

Ein neuer Mitarbeiter erhält eine freigegebene Identität und ein Facharbeitsplatzprofil. Nach erfolgreicher UZE-Prüfung und Domänenanmeldung wird ihm die zugehörige VDI zugewiesen. Die produktive Nutzung wird freigegeben, sobald die verpflichtende Baseline umgesetzt und geprüft ist.

Zusätzliche Anwendungen durchlaufen den Katalog- und Genehmigungsprozess. Bei einem Rollenwechsel werden Softwarezuordnungen und Zugriffsrechte auf Zielsysteme angepasst. Endet die Aufgabe, werden die zugehörigen Zugänge und Zuordnungen entzogen. Daten und Instanz werden gemäß den geltenden

Aufbewahrungs- und Löschregeln behandelt. Für eine spätere privilegierte Tätigkeit wird ein getrenntes PAW-Profil verwendet.

Fazit

Der automatische VDI-Prozess wird zur Grundlage eines kontrollierten Sicherheitsarbeitsplatzes. Für privilegierte Aufgaben entsteht daraus eine dedizierte PAW, deren Bereitstellung, Software und Zielzugriffe einem überprüfbaren Sollzustand folgen. sayTRUST UZE ergänzt diese Umgebung um die Isolation autorisierter Kommunikationsbeziehungen. Der Schutz entsteht aus dem abgestimmten Gesamtsystem – vom Zugriffsgerät bis zum Ziel und über den gesamten Lebenszyklus.