Zeitschrift: Bulletin Electrosuisse
Herausgeber: Electrosuisse, Verband für Elektro-, Energie- und Informationstechnik
Band: 110 (2019)
Heft: 9

Artikel: Ohne sichere Daten keine Strategie
Autor: Schlichting, Stefan
DOI: https://doi.org/10.5169/seals-855981

Ohne sichere Daten keine Strategie

Instandhaltungssysteme | Für die Gewährleistung einer sicheren Energieversorgung spielt das Schutzsystem eine entscheidende Rolle. Die Digitale Revolution verändert grundlegend die Arbeitsszenarien von Technikern, Ingenieuren und Managern in diesem Bereich der elektrischen Energieversorgung.

STEFAN SCHLICHTING ET AL.

Regelmässige Prüfungen sowie die systematische Instandhaltung und Dokumentation sind für Schutzsysteme in der Energieversorgung dringend erforderlich. Dazu bedarf es der sicheren und ergonomischen Verwaltung einer grossen Menge von Informationen beziehungsweise Daten. Dies regeln auch die neuen Normen (IEC ISO 27001/271019), nach denen EVUs als «Betreiber von kritischen Infrastrukturen» gelten. Sie müssen deshalb besondere Regeln für ihre Schutzsysteme einhalten sowie eine gute, systematische und nachvollziehbare Instandhaltungsarbeit und -dokumentation durchführen.

Instandhaltungsdaten enthalten eine Fülle von Informationen, mit denen die Verantwortlichen den Zustand der Systeme besser beurteilen und verstehen können. Sie sollten demzufolge nicht nur gespeichert, sondern auch analysiert und zur Weiterentwicklung des Schutzsystems genutzt werden.

Es zeigt sich jedoch, dass trotz aller Digitalisierungsbestrebungen weltweit viele Energieversorgungsunternehmen noch immer mit Tabellenkalkula-

Bild: Lena de Fanti/unsplash

tionsprogrammen, Papierlisten und unkoordinierten einfachsten Datenbanken für das Wartungsmanagement ihrer Schutzsysteme arbeiten. Das erschwert die Verwaltung der Datenvielfalt erheblich und ist so eigentlich auch nicht mehr konform zu den aktuellen Normen.

Weshalb das ERP-System nicht reicht

Immer wieder wird die Frage gestellt, wozu es einer speziellen Software für das Instandhaltungsmanagement von Schutzsystemen bedarf, wenn doch bereits eines der grossen bekannten ERP-Systeme installiert ist.

Die betriebswirtschaftlich und organisatorisch erforderlichen Daten über die Betriebsmittel und das Netz sind natürlich in einem herkömmlichen ERP-System vorhanden, da hierfür die entsprechenden Prozesse geschaffen wurden. Für die Arbeit mit den Schutzsystemen benötigen Techniker und Ingenieure jedoch spezielle technische Daten, deren Vorhaltung in den grossen Systemen nicht vorgesehen ist. Darüber hinaus erfolgen die Prüfungen und Wartungsaufgaben vor Ort mit Notebooks, wofür die Standard-ERP-Systeme nicht die erforderliche Funktionalität bieten.

Um sinnvoll mit den Daten eines Schutzsystems arbeiten zu können, ist wichtig, diese zunächst in Hauptkategorien zu gruppieren, welche ERP-Systeme nicht anbieten. Zum Beispiel:

- Anlagendaten
- Prüfdaten
- Relais-Einstellungen
- Instandhaltungsdaten
- Daten des Prüfmittels

Eine gute Daten-Management-Lösung sollte diese Kategorien kennen, benutzerfreundlich und trotzdem leistungsstark sein, aber auch die spezifischen Anforderungen des Betriebs und der Wartung von Schutzsystemen erfüllen. Ein geschützter Datenaustausch mit dem ERP-System stellt dann sicher, dass die in diesen Kategorien vorliegenden Anlagendaten stets auf dem neusten Stand sind. Dem Anwender bietet solch eine spezialisierte Datenbank unter anderem folgende Funktionalitäten:

- Prüfung vor Ort online und offline
- Verwaltung der Prüfdaten und Relais-Einstellungen

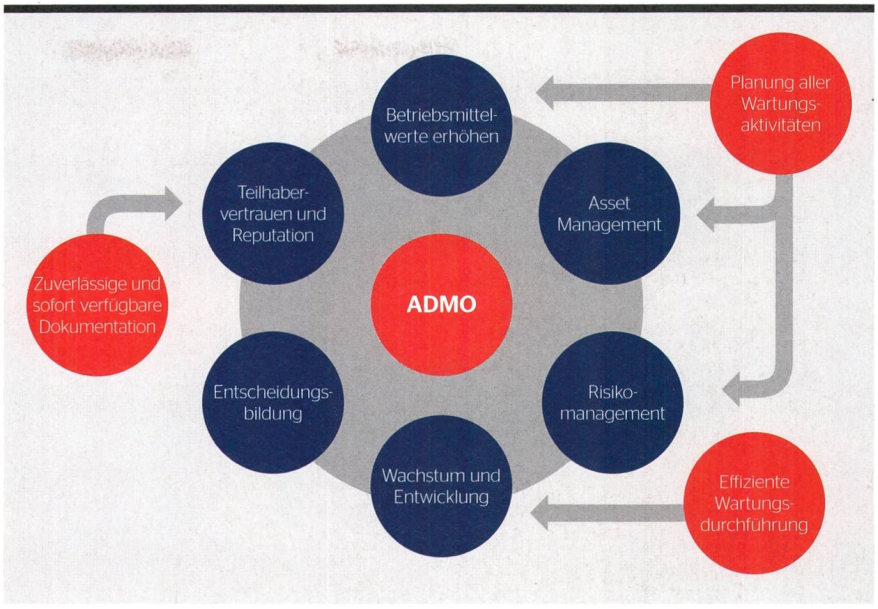

Bild 1 Die Vorteile eines integrierten Daten-Managementsystems für die technischen Anforderungen eines EVU zeigen sich vor allen Dingen in einer besseren, schnelleren, sichereren und regelkonformen Datenverwaltung.

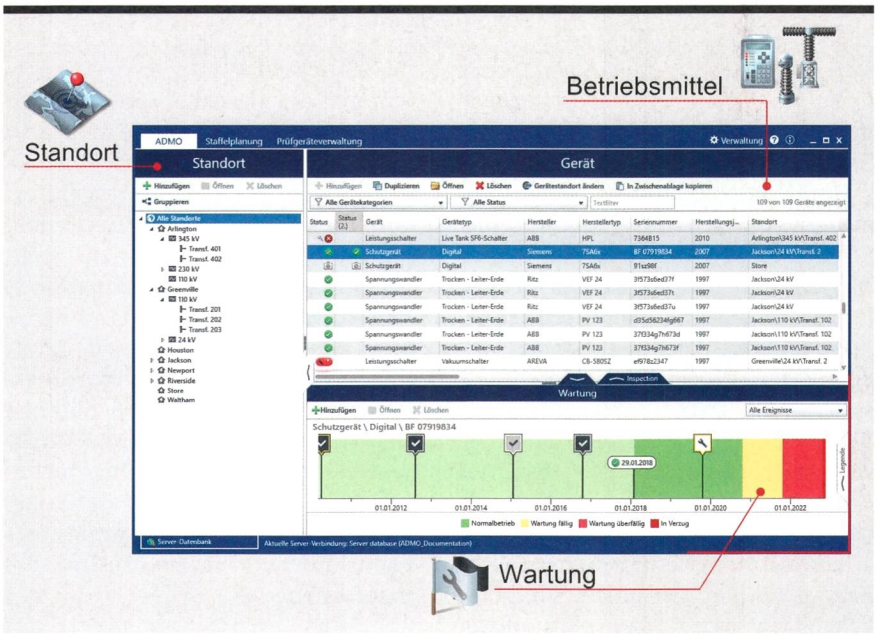

Bild 2 Die übersichtliche Organisation und sinnvolle Darstellung der im Daten-Managementsystem hinterlegten Daten ist eine der wesentlichen Grundlagen für die effiziente Wartungsplanung.

- Historie der Betriebsmittel und Gegenüberstellung
- Instandhaltungsmanagement
- Analyse des Schutzsystems

System zur Instandhaltung von Schutzsystemen

Die Grundforderungen an ein Daten-management-System, das der Instandhaltung von Schutzsystemen dient, sind einfacher Aufbau sowie einfache und intuitive Bedienung. Seine Struktur sollte die Konzepte bei der Durchführung der Prüfungs- und Wartungsaufgaben spiegeln. Zur Organisation der Systemdaten eines Schutzsystems bedarf es dreier übergeordneter Datenbereiche:

Standort: Er bildet die hierarchische Struktur des Netzes ab. Die Umspannwerke sind nach ihrer geografischen Lage gruppiert, die Spannungsebenen

Bilder: Omicron Energy GmbH

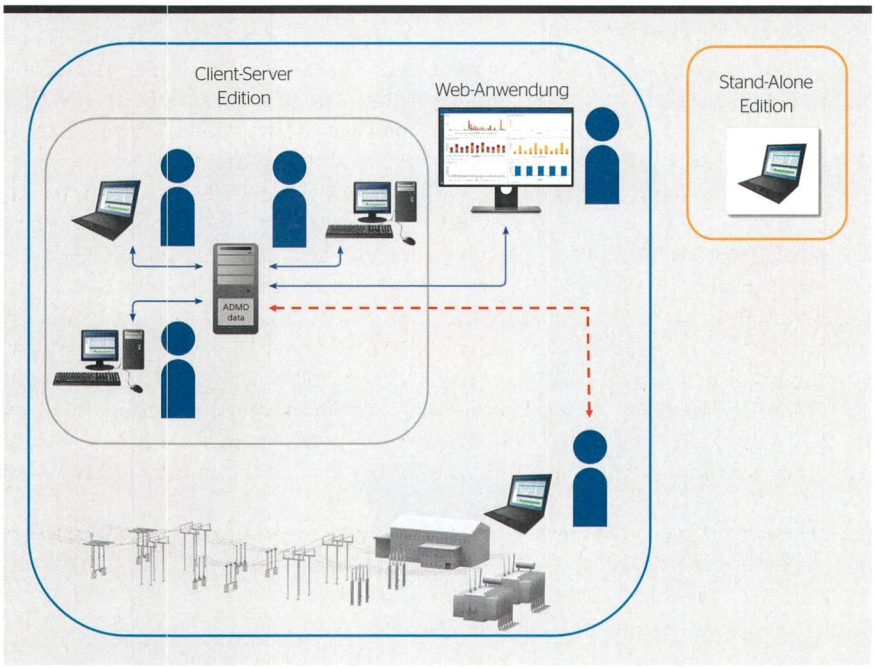

Bild 3 Für unterschiedliche Einsatzbereiche und Anforderungen stehen unterschiedliche Varianten zur Verfügung, als Einzelplatzlizenz oder als Client-Server-Version, die den Offline-Zugriff auf die Daten sowie die Datenanalyse per Web-Anwendung zulässt.

gemeinsam mit ihrer Einspeisung definiert. Dazu gehört eine Übersicht aller Betriebsmittel an diesem Standort.

Gerät/Betriebsmittel: Neben den einzelnen Schutzrelais enthält das Schutzsystem eine Vielzahl weiterer Betriebsmittel. Sie alle werden hier mit ihren technischen Daten beschrieben. Jedes Einzelne davon gehört einer vordefinierten Kategorie an und enthält spezifische Daten zum jeweiligen Betriebsmitteltyp. Da in den Umspannwerken sehr spezielle Betriebsmittel eingesetzt werden, ist es sinnvoll, mit verschiedenartigen Kategorien zu arbeiten. Eine benutzerdefinierte Kategorie bietet darüber hinaus die Möglichkeit, das ganze System so detailliert wie möglich zu beschreiben.

Wartung: Auf dieser Ebene werden die Zeitpläne und die zu jedem Betriebsmittel gehörende Zeitachse angezeigt. Hier sind speziell die Zeitpunkte für Inbetriebnahmen, Wartungen sowie andere Ereignisse und Arbeiten zu finden. Geräte mit anstehenden Wartungsaufgaben werden markiert. Dieser Bereich beantwortet auch Fragen wie

- wann erfolgte die letzte Wartung?
- wann sind die nächsten Prüfungen geplant?
- wo befinden sich die Prüfberichte für die jeweiligen Betriebsmittel?
- wie ist der aktuelle Prüf- und Wartungsstatus der gesamten Anlage?
- sind alle erforderlichen Prüfvorlagen und Prüfpläne vor Ort verfügbar?

Ein integrierter Ansatz nach dem oben beschriebenen Prinzip stellt sicher, dass sich alle Informationen stets auf dem aktuellen Stand befinden. Das System vermittelt damit einen Überblick über den Wartungszustand des kompletten Schutzsystems sowie für jede einzelne Komponente. Zum Erstellen individueller Berichte oder spezieller Analysen lassen sich die Daten in das Format eines Tabellenkalkulationsprogramms exportieren.

Client-Server-Struktur

Für den Einsatz bei Dienstleistern und kleineren EVUs ist eine Einzelplatzversion sinnvoll, die auf Notebooks läuft. Damit verwaltet ein einzelner Benutzer alle Wartungsprozesse. In den meisten Fällen arbeiten jedoch mehrere Personen in den Wartungs- und Inbetriebnahmeabteilungen der Schutztechnik und wechseln dabei ständig zwischen Büro und Aussendienst. Sie alle benötigen Zugang zu den für ihre Arbeit wichtigen Daten. Hier sollte das System als Mehrbenutzerlösung mit einer Client-Server-Struktur aufgebaut sein, das von mehreren Standorten parallelen Zugriff und synchrones Arbeiten ermöglicht. Jeder Benutzer baut dann mit seiner persönlichen ID eine sichere Verbindung zum zentralen Server auf und erhält ausschliesslich Zugriff auf die für ihn freigegebenen Daten **(Bild 3)**.

In einem Umspannwerk ist der Zugriff auf das Netzwerk oftmals nicht möglich und sollte aus Cyber-Sicherheits-Gründen für die Technik-Notebooks auch gar nicht erlaubt sein. Damit die Prüfer aber vor Ort arbeiten können, wird eine Offline-Kopie der aktuellen Datenbank auf das Notebook synchronisiert, das dann die erforderlichen Anleitungen für die jeweilige Prüfung enthält. Hierzu gehören die vorbereiteten Prüfpläne, Relais-Einstellungen, Handbücher, Schaltpläne und anderen Prüfdaten.

Während der Prüfung werden alle Prüfergebnisse in der Offline-Datenbank gespeichert und lassen sich anschliessend im Büro wieder mit dem Server synchronisieren, um sie zu analysieren oder weiter zu verarbeiten. Damit bietet dieser Ansatz sowohl für den Einsatz im Büro als auch vor Ort ein einheitliches und konsistentes Arbeitsumfeld, das die Daten für alle Benutzer stets auf dem aktuellsten Stand hält.

Analyse-Möglichkeiten

Sind die Daten des Schutzsystems vollständig erfasst und werden laufend gepflegt, können sie entsprechend ausgewertet und visualisiert werden. Um das spezielle Softwaresystem nicht mit Funktionen und Komplexität zu überfrachten, erfolgt die Analyse mit einer web-basierten Anwendung. Die Daten können damit auf jede erdenkliche Weise aus der Datenbank extrahiert und anschliessend weiterverarbeitet, analysiert und visualisiert werden. Mit Hilfe von Filtern lässt sich der Fokus auf besonders interessante Bereiche legen, beispielsweise Standorte, Spannungsebenen, Anlagentypen, Einspeisungen oder bestimmte Zeitrahmen **(Bild 4)**.

Eine Kartenfunktion **(Bild 5)** zeigt die geografische Lage der Umspannwerke in einer bestimmten Region und den jeweils zugehörigen Wartungsstatus durch farbige Markierungen. Solche Widgets und Filter lassen sich speichern und wiederverwenden.

Mit diesen Funktionen wird die Datenbank zu einem sehr mächtigen Werkzeug bei der Verwaltung des Schutzsystems. Prüfer und Planer optimieren damit ihre Instandhaltungsarbeiten und erhalten Unterstützung beim Life-Cycle-Management, Kapitaleinsatz für Betriebsmittel sowie der Personaleinsatzplanung.

Darüber hinaus ist solch ein Softwaresystem für das Instandhaltungsmanagement eine der besten Voraussetzungen für das erfolgreiche Bestehen von Audits nach den aktuellen Normen und die damit zusammenhängende vollständige Konformitätsbescheinigung.

Cyber-Sicherheit – Die «Sichere Dateninsel»

Aufgrund der Vorgaben zur IT-Sicherheit entsprechend den Normen IEC ISO 27001/271019 müssen die Systeme kritischer Infrastrukturen so aufgebaut sein, dass Büro-IT-Umgebung und die IT-Umgebung mit den technischen Daten strikt getrennt sind. Das bedeutet, dass die Instandhaltungsdaten der Schutzsysteme, ebenso wie jene für die technische Umgebung nicht direkt oder ungeschützt mit Daten der Office-Umgebung in Verbindung stehen dürfen. In den Normen wird auch der Einsatz eines systematischen Instandhaltungstools gefordert, das die Rückverfolgbarkeit von Prüfungen und Wartungsarbeiten garantiert sowie eine manipulationssichere Dokumentation zur Verfügung stellt.

Eine sichere Dateninsel ist informationstechnisch in alle Richtungen abgesichert, sodass keinerlei Zugriffsmöglichkeit besteht, ausser über einen Stammzugang, der nur berechtigten Personen oder Daten Zugang gewährt. Dieser Stamm integriert alle zentralen Leistungen, wie den Server mit den Netzwerkdaten sowie die technischen und die Instandhaltungsdaten. Von

Bild 4 Die zum gesamten Netzwerk gehörenden Betriebsmitteldaten lassen sich mit Hilfe von Filtern auf nahezu jede gewünschte Weise extrahieren, weiterverarbeiten, analysieren und visualisieren – sogar durch cybersicheren Zugriff per Web-Anwendung.

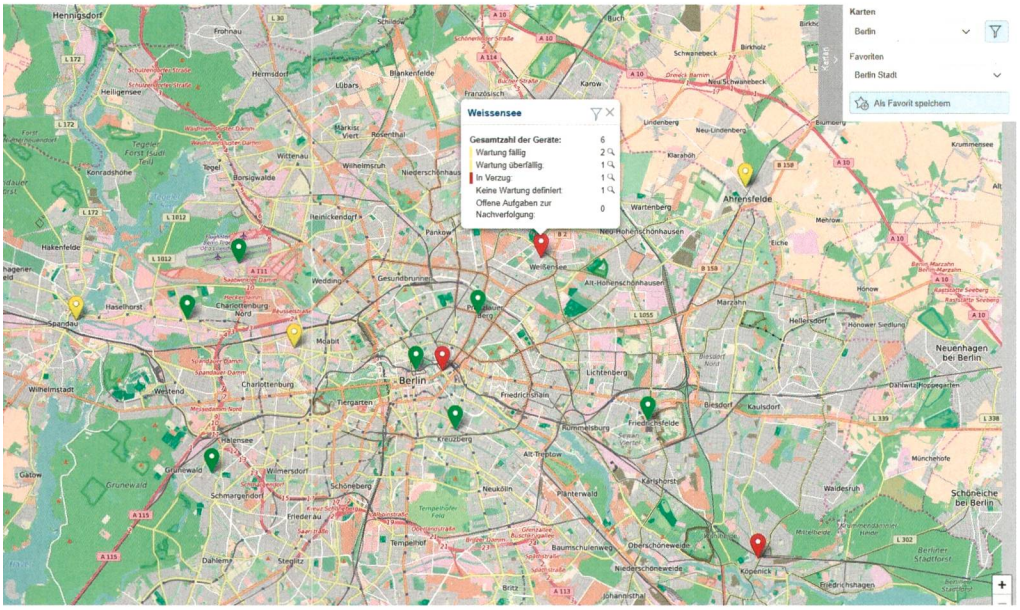

Bild 5 In der Kartenfunktion können Manager und Prüfer die geografische Lage der Umspannwerke zusammen mit einer Übersicht des Wartungsstatus der dort verwendeten Betriebsmittel erkennen.

diesem Stamm weg führen dann Verzweigungen, die die einzelnen Teile des Netzwerkes, also Orte, Umspannwerke, Betriebsmittel und alle Arbeitsmittel der Schutztechniker enthalten. Das sind all jene Bereiche, in denen technische und Wartungsarbeiten durchzuführen sind.

Integration und Austausch von Daten dürfen nur über eine sichere Datenschnittstelle erfolgen. Dazu werden die erforderlichen Daten aus dem ERP-System in das Instandhaltungssystem importiert und im Gegenzug die Wartungs- und Zustandsdaten aus der technischen Umgebung zurück in das ERP-System exportiert. Das unternehmensübergreifende ERP-System und eine spezielle Datenbank für technische Experten schliessen sich also nicht gegenseitig aus, sondern ergänzen sich vielmehr **(Bild 6)**.

Die Datenbank des Instandhaltungssystems befindet sich auf einem zentralen Server in der «Technischen Zone», also ausserhalb der üblichen Büro-IT-Umgebung und klar davon getrennt. In IT-Fachkreisen wird solch ein Bereich als Demilitarisierte Zone bezeichnet, da sie gegen Zugriffe von aussen und den üblichen Datenverkehr abgeschottet ist.

Die Benutzerkontenverwaltung regelt die jeweiligen Zugriffsrechte von Prüfern, Planern und Managern. Eine Konfliktmanagementlösung steuert den reibungslosen Zugriff. Auf diese Weise ist auch die durch die normativen Sicherheitsvorgaben geforderte Rückverfolgbarkeit für ausgeführte Arbeiten und Datenaustausch erfüllt.

Digitale Lösung ist sinnvoll

Häufig ist es sehr mühsam, den Überblick über die erforderlichen Wartungsintervalle und -termine für die Schutzsysteme zu behalten, um einen guten Zustand der zahlreichen Betriebsmittel des Schutzsystems zu gewährleisten, Prüfungen und deren Ergebnisse zu dokumentieren oder Wartungsarbeiten termingerecht durchzuführen. Bei der traditionellen Vorgehensweise mit manuellen Systemen wie Tabellenkalkulation oder Papierdokumentation sind Fehler sehr wahrscheinlich. Im Zuge der Moderni-

RÉSUMÉ

Pas de stratégie sans données sûres

Systèmes de maintenance

Des contrôles réguliers ainsi que la maintenance et la documentation systématiques sont indispensables pour les systèmes de protection dans l'approvisionnement énergétique. Pour cela, il faut une gestion sûre et ergonomique d'une grande quantité d'informations ou de données. C'est ce que règlent aussi les nouvelles normes (IEC ISO 27001/271019), qui qualifient les EAE d'« exploitants d'infrastructures critiques ». Ces entreprises doivent par conséquent respecter des règles particulières pour leurs systèmes de protection et effectuer un travail de maintenance et une documentation de celle-ci qui soient clairs, systématiques et de bonne qualité.

Les données de maintenance contiennent une abondance d'informations grâce auxquelles les responsables peuvent mieux évaluer et comprendre l'état des systèmes. En conséquence, elles devraient être non seulement stockées, mais aussi analysées et utilisées pour le développement du système de protection.

Il est souvent très laborieux de conserver la vue d'ensemble des intervalles et des dates de maintenance requis pour les systèmes de protection, pourtant nécessaires pour garantir le bon état des nombreux moyens d'exploitation du système de protection, de documenter les contrôles et leurs résultats ou d'effectuer les travaux de maintenance dans les délais. Dans la méthode traditionnelle avec des systèmes manuels tels que le tableur ou la documentation papier, il est très probable qu'il y ait des erreurs. Dans le sillon de la modernisation et avec les possibilités de la technique actuelle, il est pertinent de remplacer ces processus par une solution logicielle intégrée, qui offre aux exploitants d'infrastructures critiques un maximum de sécurité. Ainsi, ils sont en mesure de satisfaire aisément aux exigences élevées des normes et à celles liées à la cybersécurité. MR

sierung und mit den Möglichkeiten der heutigen Technik ist es sinnvoll, diese Prozesse durch eine integrierte Softwarelösung zu ersetzen, die Betreibern kritischer Infrastrukturen ein Höchstmass an Sicherheit bietet. Damit sind sie in der Lage, die hohen Anforderungen der Normen und bezüglich Cyber-Sicherheit mit Leichtigkeit zu erfüllen.

Autoren

Stefan Schlichting arbeitet im Business Development Data Management bei Omicron Electronics GmbH.
→ Omicron Electronics GmbH, A-6833 Klaus
→ Stefan.schlichting@omicronenergy.com

Stefan Schöner ist zuständig für den Bereich Data Management und Engineering Tools bei Omicron Electronics GmbH.
→ stefan.schoener@omicronenergy.com

Klaus Jotz ist Ingenieur für die Marketingkommunikation bei Omicron Electronics GmbH.
→ Klaus.jotz@omicronenergy.com

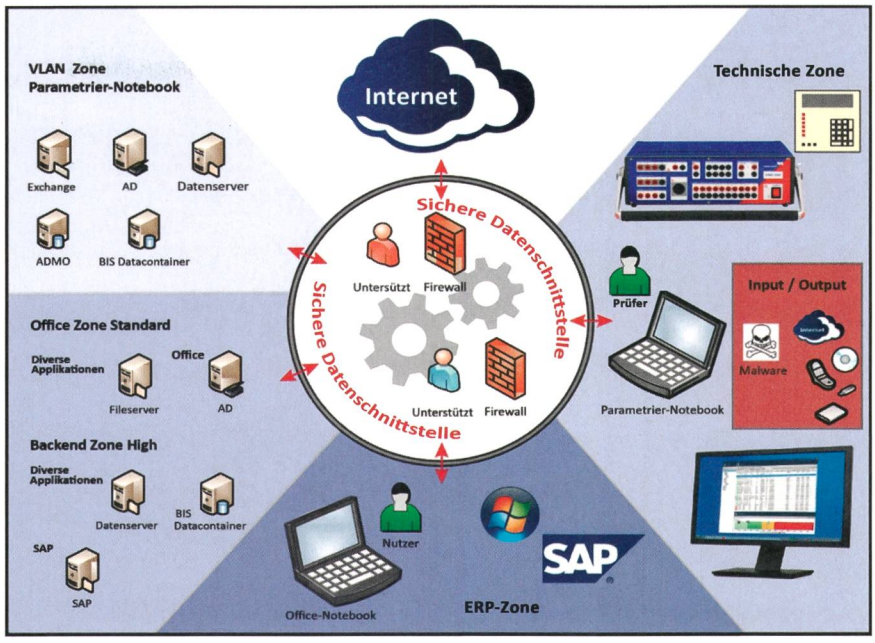

Bild 6 Der sinnvolle strukturelle Aufbau einer Datenverwaltung ermöglicht maximale Sicherheit, wie sie auch rechtlich gefordert ist – sowohl hinsichtlich des permanenten Zugriffs berechtigter Personen als auch bezüglich der Verhinderung unberechtigter Zugriffe.