Energieversorger «Verbund»

Holistischer Ansatz für SAP-Sicherheit

Der Energieversorger «Verbund» nutzt Schweizer Technologie für eine holistische Umsetzung der Compliance- und Sicherheitskonzepte seines zentralen SAP-Systems.

→ VON SALOMÉ WAGNER

DIE AUTORIN

Salomé Wagner
ist freischaffende Autorin und Kommunikationsberaterin.
→ salomewagner.com

Die Erwartungen an Betreiber kritischer Infrastruktur wie Energieversorger stehen in einem aussergewöhnlichen Spannungsfeld: Die Öffentlichkeit erwartet eine ressourcenschonende und umweltfreundliche Produktion, die sich durch Innovation und Verwendung neuer Technologien verwirklichen lässt. Mit der Digitalisierung lassen sich solche Freiräume schaffen – und dabei gleichzeitig die Sicherheit der IT erhöhen.

«Verbund» ist Österreichs führendes Stromunternehmen und einer der grössten Wasserkraft-Stromerzeuger in Europa. Bei dem Konzern stehen Innovation und Nachhaltigkeit zuoberst auf der Agenda. Das Thema Sicherheit bedeutet in diesem Kontext mehr als nur IT-Security, denn bei «Verbund» gibt es auch viele physische Sicherheitsthemen. Neben der Stromerzeugung durch Wasserkraft mit dem Unterhalt von Stauseen gibt es weitere Anlagen wie Photovoltaik und Windkraft. Daraus ergeben sich zahlreiche Interdependenzen, einerseits zwischen den Abteilungen innerhalb des Unternehmens und andererseits mit externen Partnern. Eine der wichtigsten Grundlagen für dieses Zusammenspiel ist das SAP-System, das im hoch regulierten Geschäftsumfeld hohe Anforderungen sowohl an Compliance als auch bezüglich Sicherheit zu erfüllen hat.

HOLISTISCHE SAP-SICHERHEIT

«Wir sind uns der Verantwortung bezüglich Compliance und IT-Sicherheit sehr bewusst. Zusätzlich bestehen zahlreiche Abhängigkeiten und Verbindungen zu Abteilungen bei ‹Verbund›, die natürlich in einem Rollenkonzept berücksichtigt werden müssen», sagt Thomas Zapf, Director Digitalization and Information Security bei «Verbund». Aus diesem Grund wurde das SAP-Basis-Sicherheitskonzept erweitert.

Das neue Konzept erfüllt nicht nur die sicherheits-, sondern auch die Compliance-technischen Anforderungen und Massnahmen. Die Zielsetzung konnte durch die schrittweise Projektentwicklung, die organisatorische und technische Elemente beinhaltete, erfüllt werden.

LANGJÄHRIGE KOOPERATION

Ein ganzheitliches SAP-Basis-Sicherheitskonzept umfasst nicht nur ein Sicherheitsrahmenwerk und entsprechende Dokumentation, sondern verfügt ebenso über eine leistungsfähige, technische Komponente. Bei «Verbund» ist die Software dazu neu evaluiert worden. Bei dieser Evaluation hat «mesaforte», die Governance-/Risk- & Compliance-Suite des Schweizer Anbieters wikima4, am meisten gepunktet, entsprachen sie doch auch den hohen Sicherheitsanforderungen, die es bei dem Vorhaben zu berücksichtigen galt. Inzwischen ist die Software auch im «Verbund»-Rechenzentrum implementiert, nachdem sie zuvor bei einem Partner gehostet wurde.

Der guten Grundlage und den Zielsetzungen für das Projekt geht eine lange Zusammenarbeit von «Verbund» mit den SAP-Sicherheitsexperten von wikima4 voraus. Die erste Version der Software «mesaforte» ging vor über zehn Jahren in Betrieb. Inzwischen haben sich nicht nur die regula-

«Eine homogene IT-Landschaft hilft uns, Single Points of Failure zu vermeiden»

Thomas Zapf, «Verbund»

Bild: Verbund

torischen Anforderungen an die Governance, sondern auch die Software weiterentwickelt. Die regelmässige Evaluation der Zusammenarbeit und der technischen Komponenten schafft auf beiden Seiten eine solide Vertrauensbasis.

Die bestehenden Dokumentationen von «Verbund» sind im Rahmen des Projekts in ein Sicherheitsrahmenwerk integriert worden. Dafür sind bei dem Stromkonzern gemeinsam mit wikima4 verschiedene Workshops zur Risikobewertung und deren Migration durchgeführt worden. «Die Unterstützungsprozesse zwischen den beiden Unternehmen sind etabliert», erklärt Priska Altorfer, Managing Partner von wikima4. «Dabei steht die Optimierung bestehender Konzepte und deren Umsetzung im Fokus.» Die Betriebsunterstützung, die eine laufende Anpassung der Sicherheitsmassnahmen ermöglicht, beträgt je nach Aufgabenintensität ein paar Tage im Monat. Die Projektkosten sind bei diesem Vorgehen klar kalkulierbar.

KEINE «SINGLE POINTS OF FAILURE»

Bei «Verbund» stand der pragmatische Ansatz weit oben. «Als Betreiber von kritischer Infrastruktur gibt es bei ‹Verbund› viele Sicherheitsthemen. Eine homogene Landschaft ist uns wichtig, um Single Points of Failure zu vermeiden», sagt Zapf. Aus diesem Grund steht bei der Wahl des Partners nicht nur die Software mit ihrer technischen Funktionalität im Vordergrund. Erst das Paket aus Technik und Know-how, sprich der klare Fokus auf IT-Sicherheit und entsprechende fachliche Expertise, waren ausschlaggebend. Obendrauf liefert wikima4 die unabhängige Lösung, mit der auch das Monitoring des Hosting-Partners durchgeführt werden kann.

«Die finanzielle Belastung durch die neue Software und die fallweise externe Begleitung hält sich im Rahmen», hebt Altorfer hervor. «Diese Kosten sind ständig einer Performance-Analyse unterzogen. Flexibilität ist ein weiterer Schlüssel. Die Betriebsunterstützung können wir dank langjähriger Zusammenarbeit flexibel gestalten und erreicht, je nach Aufgabenintensität, ein paar Personentage pro Monat.»

Zapf würde wieder einen gleichen Ansatz für das Projekt wählen. Unternehmen in der gleichen Situation empfiehlt er: «Wir würden den Hersteller schon bei Grundüberlegungen früher mit in die Konzeption einbinden.»

IT-SICHERHEIT IST TEAMARBEIT

Bei allen Unternehmen ist die IT-Sicherheit ein Dauerthema. Der Nutzen lässt sich nur schwer beziffern. Umso wichtiger ist das firmenweite Bewusstsein für dieses Thema, damit es auch ganzheitlich und nachhaltig im Unternehmen verankert wird. «Um die damit einhergehenden Herausforderungen bewältigen zu können, braucht es das Commitment aller Management-Stufen – sowohl von der IT als auch vom Business. Bei ‹Verbund› hat Thomas Zapf Awareness für Security geschaffen und dafür gesorgt, dass das Thema sehr breit und nachhaltig aufgestellt ist», betont Altorfer. Die interdisziplinäre Abstimmung des Know-hows wie auch der Anforderungen unter den Abteilungen ist nicht zu unterschätzen. Voraussetzung ist die gute Projektsteuerung und das reibungslose Zusammenspiel zwischen Abteilungen, dem Business, der IT mit ihrem Know-how und Umsetzungspartnern, um alle relevanten Informationen in eine harmonische Umsetzung zu bringen.

Ein nächster Schritt in Richtung ganzheitlicher Compliance und IT-Sicherheit ist die Vereinfachung bei der temporären Vergabe von Berechtigungen in SAP, besonders diejenige von kritischen Rollen. Zwei Ziele werden verfolgt: Einerseits kann das Business an Flexibilität gewinnen. Die Monate mit Home Office und die damit verbundenen, teilweise dringlichen externen Zugriffsanfragen haben die Notwendigkeit für eine flexible Lösung ins Bewusstsein gerufen. Andererseits kann sich die IT bei einer technischen Lösung neue Freiräume schaffen – und zugleich alle hohen Sicherheits- und Compliance-Anforderungen erfüllen. ←

«Verbund»-Mitarbeiter auf Kontrollgang an Europas grösstem Stadt-Kraftwerk in Wien Freudenau

«Sicherheit braucht das Commitment aller Management-Stufen – sowohl des Business als auch der IT»

Priska Altorfer, wikima4