

Kritische Infrastrukturen schützen, Souveränität sichern

HERAUSFORDERUNG

- Hohe Anforderungen an Verfügbarkeit, Resilienz und Wiederherstellbarkeit
- Fehlende Automatisierungslösungen
- Strategische Neuausrichtung mit Wechsel auf Windows 11

LÖSUNG MIT baramundi

- Co-Management für maximale Handlungsfähigkeit
- baramundi als stabiles Rückgrat für On-Prem IT-Management
- Autarker Betrieb auch ohne Internet

ERGEBNIS

- Handlungsfähig auch bei Krisen-Szenarien
- Sicherheit & Kontrolle durch zentrales IT-Management
- Sichere Verwaltung auch in abgeschotteten Netzwerksegmenten
- Digitale Souveränität durch bewusste Reduzierung von Abhängigkeiten



- Schweizer Energieversorger im Kanton Aargau
- 180 Mitarbeitende
- Betreiber von kritischer Infrastruktur (Strom, Gas, Wasser, Fernwärme)



baramundi ermöglicht genau dieses **kontrollierte Zusammenspiel von IT- und OT-Welten**, ohne Sicherheitsarchitekturen aufzuweichen oder zusätzliche Abhängigkeiten zu schaffen. Für eine kritische Infrastruktur ist das kein Komfortmerkmal, sondern ein elementarer Sicherheits- und Betriebsfaktor.“



Hybrides Endpoint Management bei der Regionalwerke AG Baden mit baramundi

Die Regionalwerke AG Baden verantwortet als Schweizer Energie- und Versorgungsunternehmen mit rund 180 Mitarbeitenden die zuverlässige Versorgung mit Strom, Gas, Wasser, Fernwärme sowie weiteren energienahen Dienstleistungen im Kanton Aargau. Als eines der ersten Elektrizitätswerke der Schweiz versorgt das regional verankerte Unternehmen seit über 125 Jahren kontinuierlich Öffentlichkeit und Industrie in Baden und Umgebung.

Oberste Priorität: Zuverlässigkeit

Mit ihrem Portfolio betreiben die Regionalwerke den Löwenanteil der kritischen Infrastruktur in ihrer Umgebung. Dementsprechend groß ist die Verantwortung, die die IT-Abteilung im Unternehmen trägt: IT-Leiter Philippe Bähler kümmert sich zusammen mit seinem zehnköpfigen Team um den stabilen, sicheren und jederzeit handlungsfähigen IT-Betrieb:

„Neben den klassischen Büroarbeitsplätzen geht es bei uns vor allem auch um die Systeme, die indirekt oder direkt Teil unserer Versorgungsprozesse sind und damit einen unmittelbaren Einfluss auf die Versorgungssicherheit haben. Verfügbarkeit, Sicherheit, Resilienz und Wiederherstellbarkeit sind für uns gelebte Realität – unter anderem geprägt durch regelmäßige Krisenstabsübungen, etablierte Notfallkonzepte und konkrete Erfahrungen aus der Energiemangel-lage der vergangenen Jahre.“

Technische und organisatorische Risiken minimieren

Vor diesem Hintergrund war die Entscheidung für ein neues Client-Management keine reine Tool-Evaluation, sondern eine strategische Weichenstellung für den langfristig sicheren und resilienten Betrieb der IT- und OT-nahen Systeme.

„Unser bisheriges Client-Management hat im Alltag zunehmend Schwächen gezeigt. Die Bedienbarkeit war sehr schwerfällig und die Software-Ergonomie war unzureichend. Schon im Client-Bereich haben wir sehr viel Zeit verloren. Zudem hatten wir im Server-Bereich keine gute Automatisierungslösung. Für mich war klar: Ein System, das im Alltag nicht intuitiv bedienbar ist, birgt langfristig Risiken. Sowohl technisch, als auch organisatorisch. Parallel dazu stand der zwingende

Wechsel von Windows 10 auf Windows 11 an. Für mich war das der logische Zeitpunkt, nicht nur das Betriebssystem zu wechseln, sondern das Client-Management grundlegend neu aufzustellen“, erklärt Bähler

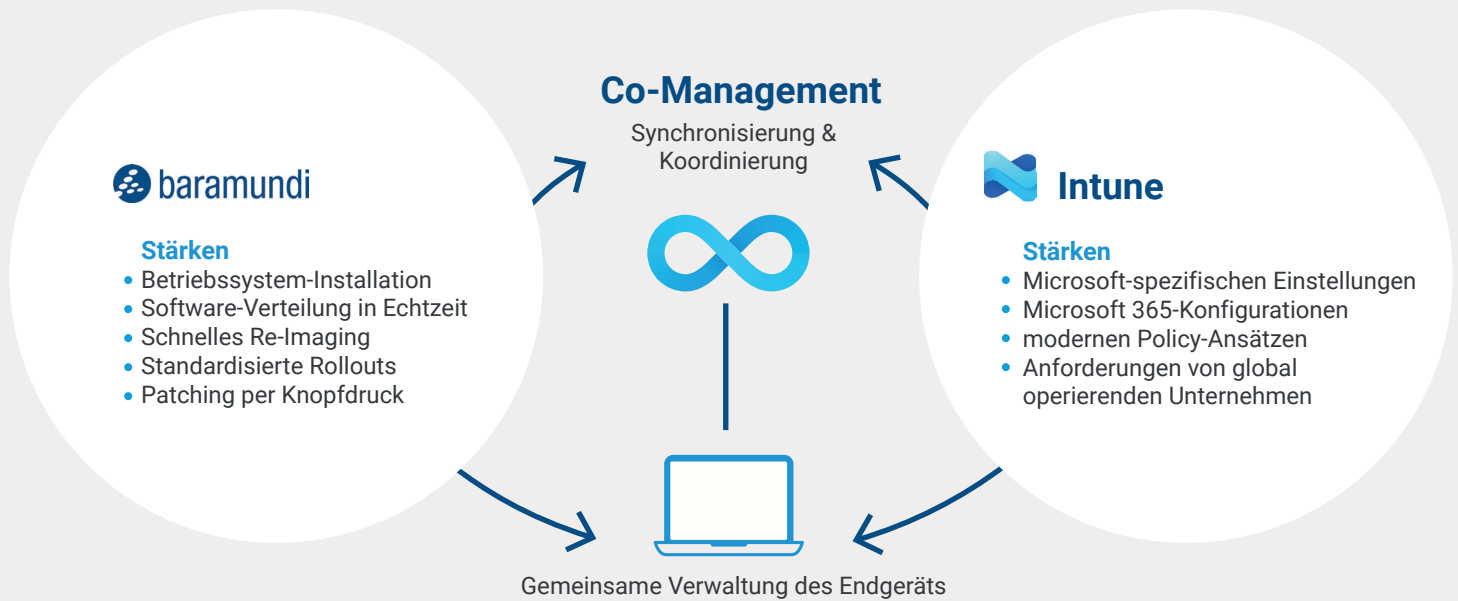
Evaluation: baramundi und Intune – kein Entweder-Oder

„Im Team gab es eine intensive Diskussion, welche Plattform wir in Zukunft verwenden sollten. Gerade jüngere Mitarbeitende haben sich für Microsoft Intune ausgesprochen. Intune ist ohne Frage ein leistungsfähiges Tool. Ich habe damit in der Vergangenheit schon einige Erfahrungen gemacht, positive wie auch kritische! Ich kannte aber auch die baramundi Management Suite aus vorherigen Anstellungen. Damit hatte ich durchgehend sehr gute Erfahrungen gemacht, insbesondere in Bezug auf Stabilität und auf Bedienbarkeit.

Ich wusste, dass baramundi ein Werkzeug ist, auf das man sich verlassen kann, insbesondere in Umgebungen, in denen Fehler nicht tolerierbar sind. Mir war aber ebenso wichtig, diesen Entscheid nicht aus Gewohnheit zu treffen. Deshalb haben wir eine strukturierte Evaluation durchgeführt und in externen Abklärungen auch den Analysten Gartner miteinbezogen.



baramundi als stabiles, schnelles Rückgrat – Intune dort, wo es fachlich Sinn macht



Unser Entscheid war daher bewusst hybrid: baramundi als stabiles, schnelles Rückgrat für Betriebssysteme, Software und Patching – Intune dort, wo es fachlich Sinn macht.“

Co-Management: Erfahrung aus der Praxis

„Spannend war für mich persönlich, dass ich bereits früher – lange bevor es offiziell so bezeichnet wurde – hybride Ansätze umgesetzt hatte: Software-Verteilung über baramundi, Einstellungen über Microsoft-Mechanismen. Damals war das noch kein offiziell supporteter Standard, funktionierte aber technisch bereits sehr gut. Während wir dieses Projekt umgesetzt haben, kam

dann die offizielle Weiterentwicklung: baramundi hat den Co-Management-Ansatz klar positioniert und technisch weiter ausgebaut. Das hat uns bestätigt, dass wir auf dem richtigen Weg sind. Im Projekt haben wir uns dann bewusst entschieden, konsequent auf Azure AD Join-only zu wechseln und nicht im klassischen hybriden AD-Modell zu verbleiben.“

Krisenfähigkeit: Handlungsfähig im Blackout

„Unsere Realität als Energieversorger sorgt dafür, dass in unseren jährlichen Krisenstabsübungen früher oder später immer dieselbe Frage gestellt wird: Was machen wir, wenn Internet oder Teile der Infrastruktur ausfallen?“



„[...] Wir haben bei der Regionalwerke AG den **Anspruch und die Verpflichtung jederzeit handlungsfähig zu sein**. Ein On-Prem System wie baramundi, das auch autark ohne Internet betrieben werden kann, bietet hier einen unverzichtbaren Vorteil.“

IT-Leiter Philippe Bähler, Regionalwerke AG Baden

Gerade in Szenarien wie:

- Blackout
- eingeschränkter Konnektivität
- Cyberangriff oder Verschlüsselung
- schnelle Wiederherstellung vieler Clients in kurzer Zeit

ist es essenziell, dass Betriebssysteme und Software lokal, schnell und unabhängig verteilt werden können. Reine Cloud- oder Online-Ansätze gelangen hier sehr schnell an ihre Grenzen.“

Patchmanagement und verschlüsselte Kommunikation – auch in abgeschotteten Zonen

„Ein weiterer zentraler Faktor war für uns die Stärke von baramundi im Bereich Patchmanagement und Sicherheit. baramundi ermöglicht ein zentrales, kontrolliertes Patchmanagement, mit dem wir jederzeit wissen:

- welche Systeme welchen Patchstand haben
- wo Sicherheitslücken bestehen
- welche Updates erfolgreich ausgerollt wurden

Besonders wichtig ist uns dabei der Sicherheitsansatz: baramundi arbeitet mit digital zertifizierten und -signierten Schlüsseln, wodurch der baramundi-Agent sicher auf Systemen installiert werden kann – unabhängig davon, ob diese:

- Mitglied eines Active Directory sind
- an Microsoft Azure AD angebunden sind
- oder bewusst komplett isoliert in sicheren Zonen betrieben werden

Damit können wir auch Systeme in abgeschotteten Netzsegmenten, in sicheren Zonen oder in OT-nahen Umgebungen zuverlässig verwalten. Die Kommunikation erfolgt über verschlüsselte, gesicherte Kanäle, ohne dass eine klassische Domänen- oder Cloud-Anbindung erforderlich ist.

Gerade im OT-Umfeld ist das für uns ein entscheidender Faktor. Dort betreiben wir Systeme, die aus Sicherheitsgründen absichtlich getrennt und stark eingeschränkt sind.

Gleichzeitig müssen diese Systeme natürlich:

- überwacht werden
- sicherheitsrelevant aktuell bleiben
- gezielt mit Updates und Konfigurationen versorgt werden

Digitale Souveränität und vermeidbare Abhängigkeiten

„Ich bin wirtschaftlich und geopolitisch interessiert und hinterfrage sehr bewusst, wo wir uns in Abhängigkeiten begeben. Nicht aus einer grundsätzlichen Ablehnung gegenüber bestimmten Anbietern, sondern aus Verantwortung. Es gibt reale Beispiele, die zeigen, dass Abhängigkeiten von einzelnen US-Anbietern in politischen oder sanktionsbedingten Situationen sehr konkrete Auswirkungen haben können. Für mich sind das reale Risiken, die ich als IT-Leiter einer kritischen Infrastruktur bewerten muss. ...



...Unser Ansatz ist deshalb gezielt ausgewogen: Microsoft-Dienste dort, wo sie fachlich sinnvoll sind, baramundi dort, wo wir maximale operative Kontrolle, Notfallfähigkeit und Unabhängigkeit benötigen. So reduzieren wir Risiken, ohne uns technologisch abzuschotten.“ *IT-Leiter Philippe Bähler, Regionalwerke AG Baden*

Fazit



*I. Caner Aslan, Senior Sales Executive baramundi,
r. IT-Leiter Philippe Bähler,
Regionalwerke AG Baden*

Die Entscheidung für die baramundi Management Suite war für uns eine klare strategische Entscheidung. Sie basiert auf:

- klaren Anforderungen aus dem Betrieb kritischer Infrastruktur
- hoher Bedeutung von Sicherheit, Patchmanagement und Verschlüsselung
- realistischen Krisen- und Notfallszenarien
- dem kontrollierten Zusammenspiel von IT- und OT-Systemen
- einer bewussten Haltung zur digitalen Souveränität



„baramundi gibt uns die Sicherheit, auch dann handlungsfähig zu bleiben, wenn andere Systeme an ihre Grenzen kommen. Genau das ist für ein Unternehmen wie die Regionalwerke AG Baden entscheidend.“