Case Study

controlware

Bachner Elektro GmbH & Co. KG.

Mit SIEM zum effizienten IT-Betrieb

Bachner Elektro erhält mit Controlware lückenlose Transparenz über die IT

Als Elektro-Dienstleister plant und realisiert die Bachner Elektro GmbH & Co. KG (im Folgenden: Bachner) für ihre Kunden anspruchsvolle Bauvorhaben und Projekte in Automobilindustrie, Luftfahrt, Krankenhäusern, Universitäten, Schulen und vielen weiteren Bereichen. Bei der Umsetzung der Projekte ist das Unternehmen auf einen jederzeit performanten und zuverlässigen IT-Betrieb angewiesen. Gemeinsam mit dem Systemintegrator und IT-Dienstleister Controlware implementierte man daher eine zeitgemäße SIEM-Plattform auf Basis von Splunk Enterprise.

Die SIEM-Plattform auf Basis von Splunk Enterprise ermöglicht es Bachner, die komplexe IT-Infrastruktur an sechs Standorten in Deutschland sowie je einem in Österreich und den USA durchgehend im Blick zu behalten und kontinuierlich zu optimieren: „Als IT-Team der Bachner Gruppe sind wir dafür verantwortlich, jederzeit einen effizienten und stabilen Betrieb unsrer über 2.000 dedizierten Systeme zu gewährleisten. Dafür müssen wir zu jedem Zeitpunkt genau wissen, was in unserer IT-Umgebung vor sich geht – und diese Transparenz hat uns lange Zeit gefehlt", erklärt Christoph Appel, Leitung IT-Administration bei Bachner. „Im Sommer 2018 haben wir uns daher entschieden, unser Monitoring und Reporting auf den Prüfstand zu stellen, und die vorhandenen Insel- und Legacy-Lösungen durch eine moderne, ganzheitliche Umbrella-Plattform für SIEM, IT-Operations und Reporting zu ersetzen. Unser Ziel war es, die Monitoring-Landschaft nachhaltig zu erweitern und betriebs- und sicherheitsrelevante Daten aus unterschiedlichsten IT-Systemen zu konsolidieren. Dies sollte das Reporting und das Troubleshooting vereinfachen und bei der Identifizierung von Verbesserungs- und Automatisierungspotenzialen helfen. Dabei war uns bewusst, wie komplex und zeitaufwendig ein solches Integrationsprojekt ist – also haben wir bereits in der Frühphase unseren langjährigen Partner Controlware hinzugezogen."

Markt-Evaluierung und Lösungsdesign

Die beiden Unternehmen analysierten gemeinsam die Assets und Anforderungen von Bachner. Anschließend definierte das Projektteam auf dieser Basis detailliert den Leistungsumfang der neuen Lösung und entwickelte ein entsprechendes Migrationskonzept.

Im Mittelpunkt der Lösung steht mit Splunk Enterprise eine der marktführenden Daten-Plattformen. Die Software übernimmt, indiziert, verarbeitet und analysiert relevante Log-Files aus den vorhandenen ATP-Plattformen, Firewalls, SD-WAN-Konsolen und Netzwerkmanagement-Appliances. Anschließend werden die Analyse-Ergebnisse grafisch aufbereitet und in individuell anpassbare Dashboards exportiert. So erhält das IT-Team von Bachner einen detaillierten Überblick über die IT-Landschaft und ist in der Lage, Optimierungspotenziale und potenzielle Schwachstellen zu lokalisieren. Neue Systeme lassen sich bei Bedarf einfach und schnell in die Lösung einbinden, ohne die Konfiguration zu ändern.

Und, wichtig für den Einsatz in der verteilten IT-Landschaft von Bachner: Splunk Enterprise ist für Multi-Cloud-Umgebungen geeignet und kann flexibel mit Splunk Cloud-Instanzen kombiniert werden, um standortübergreifende Transparenz sicherzustellen.

Mit der externen Observability-Pipeline-Lösung Cribl Stream lassen sich die Log-Daten vor dem Import in Splunk filtern, anreichern, konsolidieren und hochgradig flexibel anpassen. So können beispielsweise redundante Daten proaktiv aus dem Stream entfernt, je nach Datentyp individuelle Routing-Optionen festgelegt oder Log-Files bedarfsgerecht an die Splunk Plattform übergeben werden. Dies ermöglicht es den Anwendern, das Potenzial ihrer Investitionen optimal auszuschöpfen.

„Eine der großen Herausforderungen bei der Implementierung von SIEM-Lösungen liegt darin, die heterogenen Daten aus der IT-Landschaft in ein einheitliches und nutzbares Format zu überführen", erklärt Daniel Seifert, Pre-Sales Consultant bei Controlware. „Mit Splunk mussten wir uns nie Gedanken darüber machen, ob wir die Daten in die Plattform reinbekommen. Die Lösung ist so flexibel, dass sie mit jedem Format zurechtkommt. So lassen sich alle Logs in einer einheitlichen Plattform konsolidieren und für konkrete Use Cases nutzen."

Über Bachner Elektro GmbH & Co. KG

In über 100 Jahren Firmengeschichte hat sich bei Bachner Elektro viel bewegt. Stets wurde sich an den aktuellen Entwicklungen der Technik orientiert. Zu jeder Zeit haben die Mitarbeitenden den Fortschritt vorangetrieben und dafür gesorgt, dass die Geschichte der Bachner-Gruppe immer weitererzählt wird.

Das Leistungsspektrum wird seit über 100 Jahren stetig ausgebaut und um neueste Technologien erweitert. Das Mutterunternehmen stellt die Kernkompetenzen der Energietechnik, die Tochterunternehmen sind firm in alternativer Energieerzeugung und -speicherung sowie Kraft-Wärme-Kopplung. Die Großkunden von Bachner Elektro sind in den Zukunftsthemen zu Hause: E-Mobilität, Smart Grid und Industrie 4.0, Künstliche Intelligenz und schnelles Internet. Hier geht es besonders innovativ zu – und besonders präzise. Genau die Welt von Bachner Elektro.

Die Bachner-Gruppe agiert an 13 Standorten in Deutschland, Österreich und den USA. Derzeit werden über 700 Mitarbeitende beschäftigt, davon rund 70 Auszubildende. Verantwortung, Wertschätzung und Vertrauen prägen das Verhältnis zu Kunden und Partnern ebenso wie die Firmenkultur.

Vorkonfigurierte Use Cases

Stichwort Use Cases: Neben der Erfassung und Aufbereitung der Daten ist die Entwicklung konkreter Einsatzszenarien die zweite große Herausforderung in vielen Projekten. Gerade mittelständischen Unternehmen fällt es häufig schwer, die systematisch erfassten Log-Files in greifbaren Mehrwert zu überführen. Vielen Teams fehlt es schlichtweg an Manpower, Zeit und Erfahrung, um die eingehende Datenflut optimal zu verwerten. Daher implementierte das Projektteam auf Basis der Splunk Plattform auch die von Controlware entwickelte CESAR App. Diese erweitert Splunk Enterprise out-of-the-box um über 20 vorkonfigurierte Use Cases aus den Bereichen AD, Server, M365, Firewall, Proxy und Mail – und ermöglicht es der fünfköpfigen IT-Mannschaft von Bachner, in kürzester Zeit zuverlässige und belastbare Ergebnisse aus ihrem SIEM zu gewinnen.

Das Projektteam (v.l.n.r.): Daniel Seifert (Pre-Sales Consultant, Controlware), Reiner Altegger (Senior Business Consultant Analytics, Controlware) und Christoph Appel (Leitung IT-Administration, Bachner Elektro).

CHRISTOPH APPEL
Leitung IT-Administration,
Bachner Elektro

„Unser Ziel war es, die Monitoring-Landschaft nachhaltig zu erweitern und betriebs- und sicherheitsrelevante Daten aus unterschiedlichsten IT-Systemen zu konsolidieren."

„Controlware setzt mit der CESAR App aus unserer Sicht das i-Tüpfelchen auf ein überaus erfolgreiches Projekt – denn damit sind wir in der Lage, die meisten für uns relevanten Use Cases in einer kompakten und komfortablen App zu bündeln, und so vom ersten Tag an produktiv zu arbeiten", bestätigt Christoph Appel. „Und auch bei vielen weiteren Aufgabenstellungen – etwa beim Handling der Alarme, bei der Planung der Backups und bei der Überwachung des Compliance- und Audit-Status – ist uns die CESAR App eine große Hilfe. Bei der Definition von Use Cases arbeiten wir eng mit Controlware zusammen und wirken aktiv an der Weiterentwicklung der Anwendung mit."

Die Zukunft spricht Cloud

Seit dem erfolgreichen Go-Live der Analyse-Plattform Ende 2018 entwickeln die beiden Partner das Projekt gemeinsam kontinuierlich weiter, sowohl mit Blick auf den Rollout neuer Use Cases als auch mit Blick auf die Modernisierung des technologischen Fundaments. Letzteres muss vor allem kontinuierlich an die ansteigende Datenmenge angepasst werden – immerhin hatte sich das Datenvolumen im SIEM-Bereich bereits im ersten Jahr nach der Inbetriebnahme mehr als verdoppelt. Um die Skalierbarkeit zu erhöhen, wurde die On-Premises betriebene Splunk Enterprise Plattform daher 2021 in die Splunk Cloud migriert. Diese Cloud-basierte Variante der Lösung bietet einen nahezu identischen Funktionsumfang, kommt aber gänzlich ohne lokale Komponenten aus, und auch die Speicherung der Log-Files erfolgt vollständig in der Cloud.

Reiner Altegger, Senior Business Consultant Analytics bei Controlware, bescheinigt dem Projekt klaren Vorbildcharakter: „Wie professionell Bachner seine IT-Infrastruktur betreibt, überwacht und optimiert, ist für ein Unternehmen dieser Branche und Größe alles andere als selbstverständlich. Der durchdachte Einsatz von Use Cases und die konsequente Korrelation der Analyse-Ergebnisse ermöglichen es dem Team, einen potenziell wachsenden Mehrwert zu generieren, ohne zusätzliche Investitionen zu tätigen."

Und auch das Fazit von Christoph Appel fällt rundum positiv aus: „Das

Tolle an unserer Daten-Plattform ist, dass man keine perfekte Infrastruktur braucht, um davon zu profitieren. Im Gegenteil: Wir sind ganz einfach mit unserer bestehenden IT gestartet, und haben diese Landschaft mithilfe der Analysen in einem dynamischen und laufenden Prozess kontinuierlich optimiert und erweitert. Auf diese Weise entwickeln sich ganz automatisch neue Projekte, die neue Optimierungspotenziale ergeben."

Die IT wird zum Business-Treiber

Kein Wunder also, dass die IT-Roadmap von Bachner straff geplant ist: Aktuell fokussiert das Team um Christoph Appel vor allem die Cloud-Migration und die Office 365-Anbindung der Mitarbeiter, um die Weichen für zeitgemäße digitale Workplaces und für die Einführung neuer SaaS-Lösungen zu stellen. Und auch die turnusmäßige Evaluierung des IT-Betriebes, die 2018 den Anstoß für das SIEM-Projekt gab, steht im kommenden Jahr wieder an – gut möglich also, dass hier bereits die nächsten zukunftsweisenden Modernisierungsvorhaben initiiert werden. Kopfzerbrechen bereitet diese Aussicht Christoph Appel aber nicht: „Mit unserer Plattform-Lösung haben wir ein sehr robustes Fundament für neue Innovationsprojekte geschaffen, und können die IT besser denn je als Geschäftstreiber für unser Business nutzen. Und mit Controlware haben wir ja auch den richtigen Partner für die Umsetzung an der Hand."

Gemeinsam auf Erfolgskurs: Bachner Elektro setzt auf langjährigen Partner Controlware.

CESAR App

Aufsetzend auf der marktführenden Technologie der Splunk Enterprise Analytics-Plattform stellt die von Controlware entwickelte CESAR App Unternehmen out-of-the-box ein breites Feature-Set zur Verfügung, das von übersichtlichen Dashboards und Reports über integrierte Threat Intelligence Feeds bis hin zu flexiblen, rollenbasierten Alarm-Management- und Monitoring-Funktionalitäten reicht. Dank der vordefinierten Use Cases aus den Bereichen AD, Server, M365, Firewall, Proxy und Mail liefert die CESAR App zudem in weniger als einer Woche zuverlässige und belastbare Ergebnisse. Dabei lassen sich Reports und Alarme aus unterschiedlichen Kundenanforderungen erfassen und für die weitere Analyse bündeln.

Unsere Standorte

Zentrale
Controlware GmbH
Waldstraße 92
63128 Dietzenbach

Tel. +49 6074 858-00
Fax +49 6074 858-108
info@controlware.de
www.controlware.de
blog.controlware.de

Besuchen Sie uns auf:

Deutschland

Berlin
Tel. +49 30 67097-0
info-ber@controlware.de

Düsseldorf
Tel. +49 2159 9696-0
info-due@controlware.de

Frankfurt/Main
Tel. +49 6074 858-206
info-ffm@controlware.de

Hagen
Tel. +49 2331 8095-0
info@networkers.de

Hamburg
Tel. +49 40 251746-0
info-ham@controlware.de

Hannover
Tel. +49 511 726092-0
info-han@controlware.de

Ingolstadt
Tel. +49 841 23222-0
info-ing@controlware.de

Kassel
Tel. +49 561 47576-0
info-kas@controlware.de

Leipzig
Tel. +49 341 98387-30
info-lei@controlware.de

München
Tel. +49 89 666367-0
info-muc@controlware.de

Stuttgart
Tel. +49 711 770568-0
info-stu@controlware.de

Wolfsburg
Tel.: +49 5362 9993413
info-wey@controlware.de

Österreich

Innsbruck
Tel. +43 512 345200
info@controlware.at

Wien
Tel. +43 1 890 0724-0
info@controlware.at

Schweiz

Zürich
Tel. +49 6074 858-00
info@controlware.ch