checkmk

Case Study

Software-Hersteller überwacht KRITIS mit Checkmk

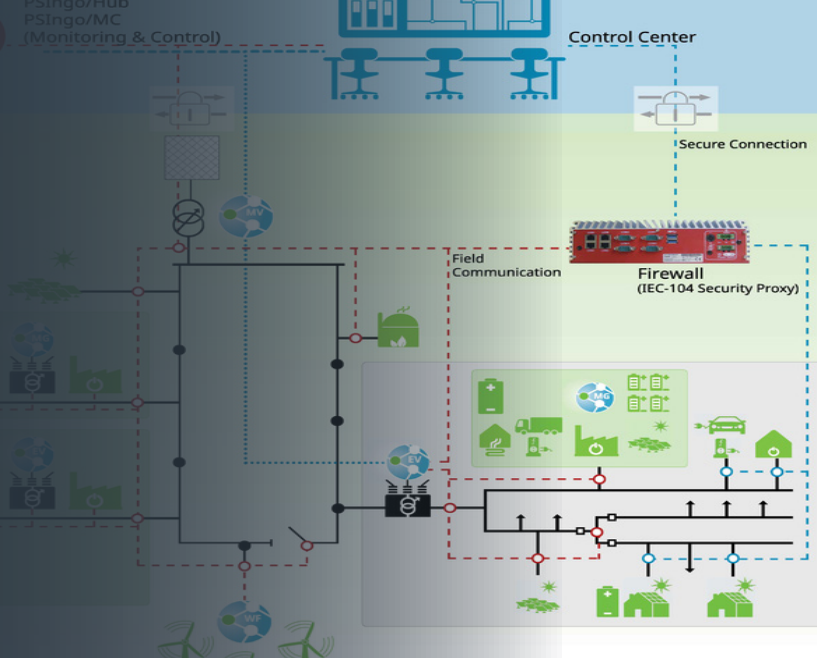
DER KUNDE

Unternehmen: PSI Software AG

Größe: 2.000 Mitarbeiter

Standort: Berlin, Deutschland

Website: www.psi.de



PSI

Der PSI-Konzern entwickelt und integriert auf der Basis eigener Software-Produkte komplette Lösungen für die Optimierung des Energie- und Materialflusses bei Versorgern und in Industrieunternehmen. Ein Teil des Angebotes beinhaltet verschiedene Managed Services, bei denen für alle eingesetzten Tools strenge Sicherheitsvorgaben beachtet werden. Je nach Branche und Kundenvorgaben müssen dabei unterschiedliche Compliance-Richtlinien umgesetzt werden.

KERNPUNKTE

- PSI vertraut seit 2017 auf die Managed Services Edition von Checkmk, um Assets bei ihren Kunden zu überwachen. Dazu gehören beispielsweise die größten Stromproduzenten Europas und Anbieter von Kritischen Infrastrukturen (KRITIS).

- Das IT-Team der PSI entschied sich für Checkmk, da es sich unter anderem dazu eignet, Assets in abgeriegelten Umgebungen zu überwachen.

- Aktuell betreibt PSI 20 Checkmk-Instanzen mit 8.000 Hosts und 60.000 Services. Das IT-Team hat das Monitoring so konfiguriert, dass es sämtliche Überwachungsdaten der Kunden regelmäßig ausschließlich per E-Mail in die zentrale Checkmk-Instanz überträgt.

SOFTWARE-PIONIER SUCHT MONITORING-TOOL

Bereits seit 1976 verzeichnet PSI Erfolge mit Software-Lösungen für Energieversorger. Seitdem ist das Unternehmen nachhaltig gewachsen, da es seine Technologien ständig optimiert und das Angebot an die Marktanforderungen anpasst. Vor dem Hintergrund steigender Sicherheitsanforderungen seitens der Kunden entschied sich PSI zum Aufbau eines Monitoring-Services und suchte dazu ein passendes Tool.

Nach intensiver Prüfung entschied sich das Unternehmen 2017 für den Einsatz der Checkmk Managed Services Edition. Als einziges Tool eignete es sich zur Erfüllung der strengen Sicherheitsvorgaben wie den KRITIS-Richtlinien nach dem IT-Sicherheitsgesetz und ist gleichzeitig in höchstem Maße flexibel bei der Übertragung der Überwachungsdaten. Zudem lässt es sich in isolierten Umgebungen lokal beim Kunden aufsetzen und ist leicht zu bedienen.

Abbildung 1: PSI überwacht Rechenzentren von KRITIS-Anbietern

Besonders wichtig ist die Möglichkeit, Monitoring-Daten per E-Mail in die zentrale Checkmk-Instanz zu übertragen. Dies ist notwendig, da sich die meisten überwachten Assets in Rechenzentren mit abgeriegelten Umgebungen befinden und diese Rechenzentren nur per E-Mail mit der Außenwelt kommunizieren können.

Der erste Schritt bei der Umsetzung ist weitgehend identisch wie in anderen Szenarien: PSI setzt im Rechenzentrum des Kunden eine Checkmk-Instanz als virtuelle Appliance auf. Dort werden IT-Assets aller Art wie Server oder Netzwerkgeräte überwacht. Für die Implementierung erhält PSI

DIE HERAUSFORDERUNG

PSI suchte eine Lösung, um Monitoring-Dienstleistungen für Energieunternehmen anzubieten. Neben den allgemeinen Anforderungen für Großunternehmen wie Skalierbarkeit und einfache Verwaltung von verteiltem Monitoring musste diese zudem strenge Vorgaben erfüllen. Dazu gehören beispielsweise das IT-Sicherheitsgesetz und interne Compliance-Anforderungen von Stromproduzenten.

die nötigen Zugriffsrechte von seinen Kunden. Die Systeme und die Überwachungsmechanismen unterscheiden sich je nach Umgebung. In der Regel setzt PSI auf die Überwachung über Checkmk-Agenten und rollt diese lokal über das Automatisierungswerkzeug Ansible aus. Zusätzlich überwacht PSI Geräte über SNMP dank den zahlreichen offiziellen Checkmk-Plugins. Außerdem nutzt das Unternehmen einige selbstgeschriebene Erweiterungen.

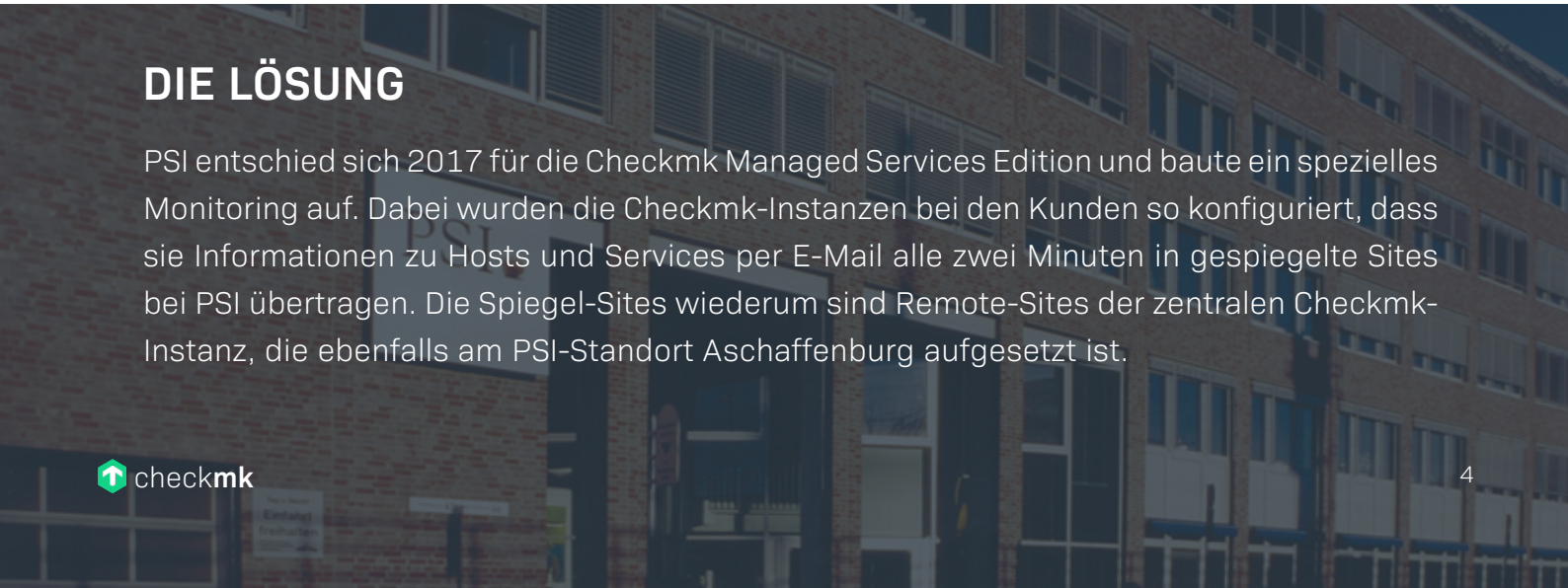
> *Die Möglichkeiten der Integrationen begeistern mich immer wieder. Der Umfang an Geräten, die integrierbar sind, ist meines Erachtens nach einzigartig in der Monitoring-Welt*
>
> **Gerald Amrhein**, System Support bei der PSI Software AG

Es sind noch einige Installationen aktiv, bei denen das IT-Team Checkmk auf SLES11 aufgesetzt hat. Der Einsatz der virtuellen Checkmk-Appliance ist jedoch wesentlich bequemer und vereinfacht Sicherheits-Audits. Zudem kann das IT-Team neue Checkmk-Versionen leichter einspielen.

MONITORING FÜR HOCHSICHERE UMGEBUNGENEN

Aktuell können Kunden-Instanzen nicht über die Livestatus-Schnittstelle mit der zentralen Checkmk-Instanz in Aschaffenburg verbunden werden. Stattdessen ermöglichte das IT-Team, dass Daten per E-Mail von den Kunden-Instanzen in die PSI-Zentrale übertragen werden können, ohne das die zentrale Instanz von außen anfragen muss.

Das IT-Team setzt dazu für jede Checkmk-Instanz der Kunden eine gespiegelte Site mit exakt den gleichen Hosts und Services in der IT-Zentrale der PSI in Aschaffenburg auf. Die Instanzen der Kunden übertragen alle zwei Minuten ihre Monitoring-Daten mittels *cmcdump*. Ein Cronjob sorgt dafür, dass die Config-Files per E-Mail an einen Mail-Server in der PSI-Zentrale gesendet



DIE LÖSUNG

PSI entschied sich 2017 für die Checkmk Managed Services Edition und baute ein spezielles Monitoring auf. Dabei wurden die Checkmk-Instanzen bei den Kunden so konfiguriert, dass sie Informationen zu Hosts und Services per E-Mail alle zwei Minuten in gespiegelte Sites bei PSI übertragen. Die Spiegel-Sites wiederum sind Remote-Sites der zentralen Checkmk-Instanz, die ebenfalls am PSI-Standort Aschaffenburg aufgesetzt ist.

werden. Ein *fetchmail* extrahiert die E-Mails anschließend aus dem Inbox-Ordner für die weitere Verarbeitung. Ein Bash-Skript erkennt über den Namen des Kunden in der Betreffzeile die passende Spiegel-Site und spielt die Monitoring-Daten auf der passenden Checkmk-Instanz ein. Der Ansatz funktioniert, da Checkmk nie auf eine zentrale Datenhaltung angewiesen und flexibel bei der Verarbeitung von Input ist.

Die gespiegelten Sites befinden sich in einem segmentierten Netzwerk zusammen mit der Zentral-Instanz. Daher ist hier jetzt ein verteiltes Monitoring mit Livestatus möglich. Alle Informationen laufen in der zentralen Checkmk-Instanz zusammen. PSI hat so alle Details im Blick und kann umgehend auf Zwischenfälle reagieren. Die komplette E-Mail-Kommunikation ist über PGP durchgängig verschlüsselt. Die nötigen Skripte hat das IT-Team selbst geschrieben.

Aktuell laufen in der Zentral-Instanz Daten aus 20 Rechenzentren von mehr als 10 Kunden aus dem Energiesektor zusammen. Insgesamt überwacht PSI 8.000 Hosts und 60.000 Services. Die Mail-Server verarbeitet täglich 15.000 E-Mails.

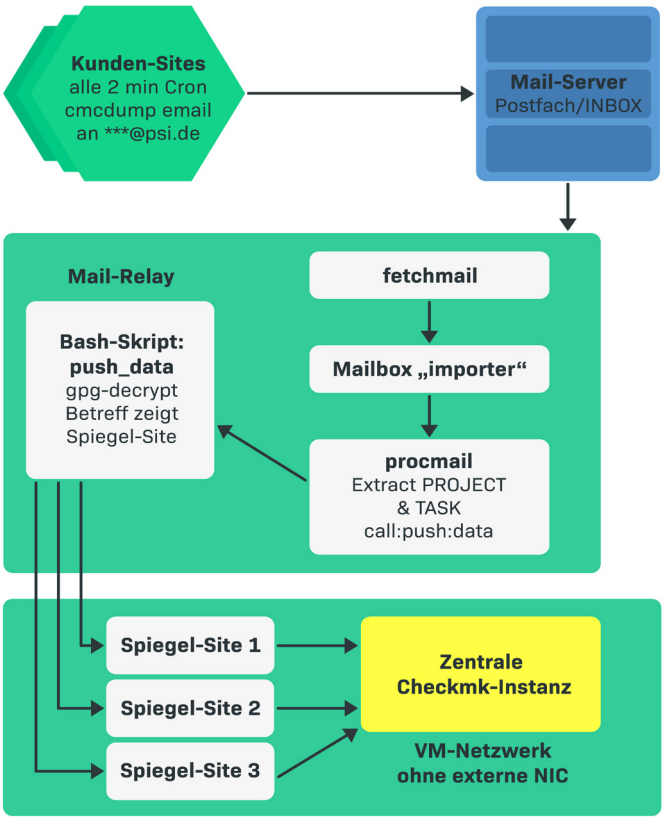


Abbildung 2: Aufbau des verteilten Monitorings über E-Mail

Die Freigabe von Leserechten ermöglicht es jedem Kunden, seine Assets einzusehen und schafft so Transparenz. Die Managed Services Edition von Checkmk erlaubt die sichere Trennung der Kundendaten und schützt vor ungewollten Zugriffen.

DIE VORTEILE

PSI hat ein einzigartiges Service-Angebot geschaffen. Trotz Abriegelung und unter Beachtung höchster Sicherheitsanforderungen der überwachten Infrastruktur hat das IT-Team jederzeit die volle Übersicht und kann schnell selbst auf kleinste Anomalien reagieren. Die IT-Experten haben alle Werte im Blick und können effizient Maßnahmen einleiten, falls es nötig sein sollte.

INTEGRATION VON WEITEREN STANDORTEN IST IN ARBEIT

Die Übertragung per E-Mail funktioniert sehr gut und bietet den Kunden einen großen Mehrwert. Das IT-Team muss nicht ständig vor Ort sein und hat trotzdem jederzeit den Überblick. PSI arbeitet an der Integration von zehn weiteren Kunden-Standorten und möchte das Monitoring um neue Systeme erweitern.

> *Ich bin froh, dass wir so kritisch bei der Auswahl des Monitoring-Tools waren. Mit Checkmk sind wir für Audits und neue Herausforderungen sehr gut aufgestellt.*
>
> **Gerald Amrhein**, System Support bei der PSI Software AG

Beispielsweise plant PSI die Überwachung von Steuerungsmodulen ihrer Kunden. Diese kann Checkmk über SNMP überwachen, allerdings befinden sich solche Assets in der Regel in anderen Netzwerksegmenten. Daher arbeitet das Software-Unternehmen an einem Proxy-Server, der als eine Art sicheres SNMP-Relay dient.

Abbildung 4: Die größten Energieunternehmen Europas vertrauen auf PSI

Eine weitere Herausforderung ist die Umsetzung des eigenen Information Security Management System (ISMS)-Prozesses, um die Zertifizierung nach ISO-27001 sicherzustellen. Hier ist das IT-Team im Austausch mit dem internen Compliance-Beauftragten. Die Anforderungen sind hoch, durch die Erfahrung der PSI-Mitarbeiter und die Anpassungsfähigkeit von Checkmk kommt die Umsetzung aber gut voran.

Pressekontakt:
tribe29 — the check**mk** company
Kellerstraße 29
81667 München

E: info@tribe29.com
T: +49 89 9982 097 00