

BayWa

Beobachtungsservice im Minutentakt – führender deutscher Konzern für Agrar, Bau und Energie sorgt mit Symantec für noch mehr Sicherheit

Auch im Agrar-, Bau- und Energie-Geschäft sind die Datennetze „business critical“. Sie müssen zuverlässig verfügbar sein – an 365 Tagen im Jahr, rund um die Uhr. Beim BayWa-Konzern setzt man daher nicht nur auf Abwehrsysteme, sondern auch auf eine professionelle Überwachung. Der verantwortliche IT-Provider Ri-Solution GmbH engagierte dafür den externen Dienstleister seines Vertrauens, das Security Operations Center (SOC) von Symantec. Er überprüft die Log Files im Minutentakt und untersucht Auffälligkeiten. Bei Gefahr schlagen die Symantec-Experten Alarm, so dass umgehend reagiert werden kann.

Wissen, was los ist

Was besonders wertvoll ist, wird in der Regel nicht nur gut gesichert, sondern auch gründlich bewacht. Daher gibt es etwa in Museen, öffentlichen Gebäuden oder Forschungszentren nicht nur Alarmanlagen, sondern zusätzlich Wachpersonal. Ganz ähnlich verhält es sich bei IT-Infrastrukturen. In zahlreichen Unternehmen werden sie nicht nur durch Firewall und Intrusion-Detection- und Prevention-Systeme gesichert, sondern außerdem rund um die Uhr aktiv überwacht. So auch bei der BayWa, dem bayerischen Traditionskonzern. Seit 1923 steht der Lieferant für Agrarprodukte im Dienste der heimischen Landwirtschaft. Mittlerweile versorgt das Unternehmen Kunden weltweit mit Agrargütern, Baustoffen, Energie und angrenzenden Dienstleistungen.

Etwa 8.500 BayWa-Mitarbeiter sind an deutschlandweit rund 700 Standorten beschäftigt. Für deren IT-Infrastruktur verantwortlich ist die Ri-Solution GmbH, deren Bereich Kommunikationstechnik unter Leitung von Andreas Maurer die Datennetze der BayWa und deren Sicherheit verantwortet. Wie in vielen anderen Unternehmen ist auch bei der BayWa das Funktionieren der Datennetze geschäftskritisch. So etwa muss die E-Mail-Applikation stets verfügbar sein – 24 Stunden am Tag und sieben Tage in der Woche. Daher ist weitreichender Schutz oberstes Gebot. „Zum guten Schutz der Datennetze zählen für uns die laufende Überwachung der Log-Files und deren effektive Auswertung“, so Andreas Maurer, „damit man Angreifer zuverlässig und rasch identifizieren kann – möglichst ohne Fehlalarme auszulösen. Und das leisten externe Sicherheitsexperten besser als wir.“ Denn Symantec erfasst täglich Daten aus über zwei Millionen eigens zu diesem Zweck eingerichteten E-Mail-Konten, 150 Millionen Desktop-Virenschutz-Sensoren sowie 40.000 Intrusion-Detection- und Firewall-Sensoren weltweit. Auf dieser Basis aktualisieren die Symantec-Sicherheitsexperten ständig ihr Bild der aktuellen Bedrohungslage. Eine Leistung, die in

„Unser Ziel war ehrgeizig, wir wollten nicht nur die Sicherheit erhöhen, sondern auf diesem Weg außerdem auch Kosten sparen.“

Andreas Maurer

Leitung Bereich
Kommunikationstechnik,
Ri-Solution GmbH

Unternehmen

Ri-Solution GmbH, der IT-Provider der BayWa AG

Unternehmensprofil

Der international tätige BayWa-Konzern hat seinen Schwerpunkt in den Bereichen Groß- und Einzelhandel sowie Dienstleistungen. Die Geschäftsaktivitäten der 1923 gegründeten Muttergesellschaft BayWa AG teilen sich auf in die Segmente Agrar, Bau und Energie. Weitere Konzerngesellschaften befassen sich mit Konsumgüterproduktion und Autohandel. Der Konzern hat inklusive Franchise- und Partnerfirmen rund 2.625 Vertriebsstandorte in acht europäischen Ländern. Die Hauptvertriebsgebiete liegen in Deutschland, Österreich und Osteuropa.

Branche

Groß- und Einzelhandel sowie Dienstleistung in den Bereichen Agrar, Bau und Energie

Symantec Services

Symantec Monitored Services

„Symantec bündelt das Wissen um die aktuellen Angriffsmuster minutenaktuell. Damit sind wir auch gegen Angreifer gewappnet, die versuchen, mit neuesten Methoden in unser Unternehmensnetz einzudringen.“

Andreas Maurer

Leitung Bereich Kommunikationstechnik,
Ri-Solution GmbH

dieser Form nur ein weltweit tätiges Expertenteam erbringen kann.

Vor diesem Hintergrund entschied sich Ri-Solution im Jahr 2004, diesen Service auszulagern. „Unser Ziel war ehrgeizig“, erinnert sich Maurer, „wir wollten nicht nur die Sicherheit erhöhen, sondern auf diesem Weg außerdem auch Kosten sparen.“ Statt eines eigenen, teuren Sicherheitsdienstes mit Einsatzzeiten rund um die Uhr hat Ri-Solution den Überwachungsdienst vollständig ausgelagert. Nun sind die Kosten präzise kalkulierbar und spürbar gesunken. Die eigene Mannschaft kann sich auf andere wichtige Aufgaben konzentrieren. Denn nachts haben die Ri-Solution-Mitarbeiter lediglich Bereitschaftsdienst.

Auffälligkeiten im Netz, so können zeitnah neu auftretende Schadcodes identifiziert und in der Symantec-Datenbank erfasst werden. Dieses Archiv bildet die Grundlage für die Überwachung der Ports. Jede an einem Port festgestellte Auffälligkeit wird mit aufgezeichneten oder neu erkannten Angriffsmustern verglichen. Stellt man die Übereinstimmung eines solchen Musters mit einem Schadcode – und damit eine potenzielle Gefahr für die betroffenen Firmennetze – fest, schlagen die Sicherheitsexperten von Symantec Alarm. „Symantec bündelt das Wissen um die aktuellen Angriffsmuster minutenaktuell. Damit sind wir auch gegen Angreifer gewappnet, die versuchen, mit neuesten Methoden in unser Unternehmensnetz einzudringen“, erklärt Maurer.

Beobachtungsservice im Minutentakt

Das redundant aufgebaute Rechenzentrum von Ri-Solution verwaltet die Daten der über 700 Standorte der BayWa AG. Mittels Spiegelung und Cluster gewährleistet es eine hohe Ausfallsicherheit. Zusätzliche Sicherheit bietet die laufende Überwachung der Ports durch das Symantec Security Operations Center (SOC). Insgesamt verfolgen rund 135 Spezialisten weltweit

Im SOC werden alle Bewegungen lückenlos erfasst: In einem Takt von fünf Minuten zeichnet man die Log Files der betreuten Unternehmen auf und überträgt sie in eines der SOC-Netze. Dort übernimmt die SOC-Technologie mit ihrem einzigartigen Auswertungssystem die Log-File-Daten. Diese werden zunächst in einen einheitlichen, vom Sicherheitssystem des Kunden unabhängigen Duktus gesetzt.

DIE LÖSUNG AUF EINEN BLICK

Die Herausforderung

Schutz der System-Infrastruktur vor externen Bedrohungen durch 7x24-Überwachung mit höchster Qualität.

Die Lösung

Symantec Monitored Services für IPS Cluster und Firewall Cluster bietet Überwachung im Minutentakt. Auffälligkeiten werden untersucht. Sobald die Symantec-Sicherheitsexperten eine Gefahr feststellen, schlagen sie Alarm.

Kaufmännische Ziele

- Erhöhte Sicherheit der IT-Infrastruktur
- Realisation von Kosteneinsparungen durch Outtasking

Technische Ziele

Echtzeitschutz im Hinblick auf neue Angreifer, interne Probleme oder ein verändertes Bedrohungsszenario

Beauftragter Symantec-Service

Symantec Monitored Services, Teil der Symantec™ Managed Security Services

Anschließend prüft die SOC-Technologie die Daten auf Auffälligkeiten, wobei es auch kleinste Abweichungen registriert.

Überwachung für die Überwacher

Andreas Maurer setzt bei der Frage nach der bestmöglichen Überwachung seiner Systeme nicht nur auf die Expertise des Symantec-SOC – sondern außerdem auf eigene Kontrolle: Einmal jährlich beauftragt er einen Hacker, das System von Ri-Solution anzugreifen. Mit modernsten Methoden, zu verschiedenen, Maurer selbst unbekanntem Zeitpunkten. Bisher waren die Auftrags-Hacker ohne Erfolg – denn Symantec konnte dank seines ausgereiften Überwachungssystems sämtliche Angriffe frühzeitig identifizieren und effektiv abwehren. „Das SOC hat sämtliche Auftragsangriffe

rechtzeitig entdeckt“, freut sich Andreas Maurer.

Auswahlkriterium „Vertrauenswürdigkeit“

„Als wir im Jahr 2004 nach einer geeigneten Lösung suchten, hatte die Vertrauenswürdigkeit des Anbieters oberste Priorität“, erinnert sich Maurer. Den Zugriff auf die Log Files des Konzerns wollte man nur einem externen Dienstleister gewähren, der eine solide Marktposition und höchste Professionalität vorweisen konnte. Daher fiel die Wahl auf Symantec. Seither sind die Experten von Symantec rund um die Uhr für die BayWa tätig. So effizient und erfolgreich, dass in diesem Zeitraum die Abteilung zwar monatlich etwa einen Alarm, aber keinen gefährlichen Sicherheitsvorfall zu verzeichnen hatte. ■

„Als wir im Jahr 2004 nach einer geeigneten Lösung suchten, hatte die Vertrauenswürdigkeit des Anbieters oberste Priorität.“

Andreas Maurer

Leitung Bereich Kommunikationstechnik,
Ri-Solution GmbH