KUNDENREFERENZ

IS4IT

Das Security Operations Center der IS4IT-Gruppe als Lösung für den Maschinenbau

WENN SICHERHEIT UNVERZICHTBAR IST

Für international agierende Maschinenbau-Unternehmen sind umfangreiche Schutzmaßnahmen in Zeiten von sich stetig ändernden Cyberattacken unabdingbar. Sie sind ein potenzielles Ziel von organisierter Kriminalität, Industriespionage und auch für Hacker verschiedener Länder von Interesse. Zum Maßnahmenpaket einer Branchengröße, die maximale Sicherheitsstandards anstrebt, gehört daher als wesentlicher Faktor ein Security Operations Center (SOC), das als Managed Security Service von der IS4IT-Gruppe betrieben wird.

Wie hoch das Bewusstsein für Informationssicherheit in diesem Unternehmen ist, zeigt sich u. a. darin, dass das Thema SOC nicht wie üblich im IT-Betrieb, sondern beim CISO organisatorisch aufgehängt ist und von diesem aktiv vorangetrieben wird.

Das weltweit an über 30 Standorten tätige Unternehmen beauftragte die IS4IT-Gruppe mit einer Analyse der IT-Infrastruktur in Bezug auf die Informationssicherheit. In mehreren Workshops wurden verschiedene Aspekte der Informationssicherheit betrachtet und mit den Verantwortlichen besprochen. Die Ergebnisse dienten zur Klärung der grundlegenden Sicherheitssituation und boten Ansätze zur Optimierung des Sicherheitsniveaus und der Sicherheitsstandards. Gleichzeitig waren sie Vorbereitung für die zielgerichtete und zeitlich abgestufte Implementierung des Security Information and Event Management (SIEM) auf dem der Managed SOC Service der IS4IT basiert.

Um dem aktuell hohen Risiko in der Cybergefährdungslage entgegenzutreten, wollte man sich zunächst auf die Identifikation illegitimer Zugangswege fokussieren. Anschließend sollten sämtliche Systeme verstärkt überwacht werden, die aufgrund ihrer Architektur eine signifikante Angriffsfläche nach außen bieten. Danach standen die Überwachung externer Ressourcen und regelmäßige Vulnerability Scans von geschäftskritischen Komponenten auf dem Plan.

Um das alles effizient und wirtschaftlich umzusetzen, entschied man sich für die Zusammenarbeit mit der IS4IT-Gruppe.

> Mit der professionellen Einführung eines **Managed SOC** durch die IS4IT konnte das **Sicherheitsniveau** unseres Unternehmens nicht nur gehalten, sondern auch signifikant **verbessert** werden. Partnerschaftlich wurden die Anforderungen definiert, in einem **PoC/PoV** validiert und danach erfolgreich implementiert. Das Managed SOC stellt seitdem einen wichtigen Pfeiler der **Informationssicherheitsarchitektur** unseres Unternehmens dar. Durch die kontinuierliche Weiterentwicklung des Managed SOC und die Anpassung an neue Gegebenheiten hat die IS4IT ihre Möglichkeiten eindrucksvoll unter Beweis gestellt.
>
> *Chief Information Security Officer (CISO), Maschinenbau-Unternehmen*

ANFORDERUNGEN

- Umsetzung hoher Sicherheitsmaßnahmen
- Frühzeitige Angriffserkennung zur Schadensminimierung
- Vermeidung von Sicherheitsfällen
- Schutz vor Hackerangriffen
- Schutz vor internen Bedrohungen und Industriespionage
- Steigerung des Sicherheitsniveaus

LÖSUNGEN

- Managed SOC Service
- Managed SIEM Service
- Vulnerability Scanning

NUTZEN

- Aufbau einer skalierbaren Sicherheitsarchitektur sorgt für ein konstant hohes Sicherheitsniveau
- Auf die eigenen Anforderungen zugeschnittene Sicherheitskonzeption
- Zuverlässige Sicherstellung der Angriffserkennung
- Schnelle Erkennung von Konfigurationsfehlern
- Wirtschaftliche Umsetzung durch Outsourcing
- Generelle Erhöhung des Reifegrads im Systembetrieb
- Outsourcing schafft Raum für wichtige Kernaufgaben der eigenen Mitarbeiter
- Synergieeffekte durch Wissen aus anderen Unternehmen

Vom Proof of Concept (PoC) zum Regelbetrieb

Bereits im PoC wurden die Nutzenpotenziale der Zusammenarbeit mit dem Managed SOC Team und dem Einsatz des SIEM-Systems, aber auch die Komplexität der Umgebung deutlich. Bei einer sehr großen Anzahl Events und Flows pro Minute tagsüber und einem enorm hohen zu verarbeitenden Datenvolumen ist ein Security Monitoring ohne ein SIEM-System nicht realisierbar. Denn selbst wenn ein SIEM-System keine Angriffe verhindert, kann man auf diese dank frühzeitiger Erkennung schnell reagieren und damit die möglichen Auswirkungen spürbar minimieren – ganz gleich, ob es um Unregelmäßigkeiten im Netzwerk, ungewöhnlichen Datenverkehr, außergewöhnliches Nutzerverhalten oder das Aufspüren von Malware-Aktivitäten geht.

Aber nicht nur in Bezug auf Sicherheitsaspekte lagen die Vorteile des SIEM-Systems auf der Hand. Der PoC machte deutlich, dass dadurch der Reifegrad des Systembetriebs insgesamt erhöht werden kann. Er erkennt unvollständige oder mangelhafte Server und Fehler in der Konfiguration der Netzwerkkomponenten und überwacht die Einhaltung der Administrationsvorgaben. Die höhere Stabilität und Qualität des Betriebs wirken sich direkt positiv auf das Niveau der Informationssicherheit aus. Dadurch werden auch Compliance-Vorgaben optimal adressiert.

Kontinuierliche Weiterentwicklung für maximale Sicherheit

Der Regelbetrieb startete im Januar 2022 und die Ergebnisse spiegeln die Erwartungen wider. Die Schutzsysteme wurden durch den Kunden so konfiguriert, dass unzulässige Verbindungen gar nicht zugelassen werden. Auch hierbei unterstützen Mitarbeiter der IS4IT-Gruppe. Wöchentliche Vulnerability Scans sorgen dafür, dass Schwachstellen nicht lange unerkannt bleiben.

Das Unternehmen zieht die IS4IT bei Fragen zur Informationssicherheit regelmäßig zurate. Gemeinsam mit dem CISO wird die Sicherheitsarchitektur sukzessive weiterentwickelt und ausgebaut. Eine Grundlage bilden umfassende Berichte, die teilweise speziell für den CISO angefertigt werden. In kontinuierlichen technischen und organisatorischen Review-Meetings wird die aktuelle Situation kritisch hinterfragt und es werden neue Anforderungen festgelegt. So wird das hohe Sicherheitsniveau, das das Unternehmen durch das Managed SOC der IS4IT-Gruppe erreicht hat, nicht nur erhalten, sondern konsequent gesteigert.

ÜBER DEN KUNDEN

Branche: **Maschinenbau**

Mitarbeiter: **über 4.000**

IS4IT

Der digitalen Souveränität verpflichtet.

IS4IT GmbH
Grünwalder Weg 28b
82041 Oberhaching
telefon +49 89 6389848-0
info@is4it.de
www.is4it.de