

Zuverlässige Cybersicherheit
durch das 8com SOC
bei einem führenden,
europäischen
Möbelunternehmen
(Herstellung und Handel)





Der Kunde

Der Kunde ist ein führendes, europäisches Unternehmen für Design, Produktion und Handel mit Wohn- und Büromöbeln, weltweit vertreten mit Niederlassungen und Schauräumen. Es beschäftigt ca. 700 Mitarbeitende und erzielt einen Jahresumsatz von mehreren hundert Millionen Euro.

8com

Die 8com GmbH & Co. KG hat ihren Sitz in Neustadt an der Weinstraße. 2004 von Götz und Sandra Schartner gegründet, sind aktuell 110 Mitarbeitende dafür verantwortlich, die Cyber-Resilienz von mehr als 115 Kunden in über 40 Ländern zu stärken. 8com schützt Unternehmen vor Cyberangriffen, rund um die Uhr im Schichtbetrieb, direkt vor Ort in Deutschland – und das seit 20 Jahren! Die Kernprozesse des SOC – einem der modernsten in ganz Europa – sind nach BSI IT-Grundschutz zertifiziert.



Ausgangslage

Das Unternehmen hatte es sich zum Ziel gesetzt, der zunehmenden Bedrohungslage im Bereich der Cyberkriminalität gerecht zu werden und seine immer komplexer werdende IT-Sicherheitsinfrastruktur transparent und effizient zu managen.

Dies war ein Grund, warum das Unternehmen einen Managed SOC Service in Anspruch nehmen wollte. Die Entscheidung fiel auf das Security Operations Center (SOC) der 8com. Ziel war es, den Schutz sensibler Daten zu gewährleisten, Ausfallrisiken zu minimieren und unternehmensinterne IT-Ressourcen zu entlasten – mit 8com als erfahrenem, zuverlässigem SOC-Dienstleister und Partner in Sachen Cyber Security.



✓ Herausforderungen

Vor der Beauftragung eines externen SOC stand das Unternehmen vor einer Vielzahl von Herausforderungen. Besondere Priorität hatte die Sicherung wertvoller Patente und Produktionspläne, da ein Sicherheitsvorfall verheerende Auswirkungen auf die Wettbewerbsfähigkeit des Unternehmens hätte. Darüber hinaus galt es, die Betriebsabläufe an mehreren internationalen Standorten abzusichern, um Produktionsstillstände zu vermeiden und die Lieferketten aufrechtzuerhalten. Das Unternehmen strebte insgesamt einen umfassenden Service an, der die gesamte Sicherheitskultur des Unternehmens stärkt.

Ziele des Kunden

Mit der Beauftragung von 8com verfolgte das Unternehmen klare Ziele:

 **Entlastung der internen IT-Abteilung**

Durch die Übergabe der Cybersicherheitsüberwachung an 8com sollte sich das IT-Team wieder auf seine Kernaufgaben konzentrieren können. Die Verantwortlichen wollten „nachts wieder ruhig schlafen“ und sicher sein, dass ihre Systeme und sensiblen Daten 24/7/365 bestens geschützt sind.

 **Absicherung der Betriebsabläufe**

Der Schutz der Produktionsstätten und der reibungslose Ablauf von Fertigung und Logistik sollten gewährleistet sein, um finanzielle und operative Risiken zu minimieren.

 **Stärkung der Sicherheitskultur**

Das Sicherheitsbewusstsein sollte im ganzen Unternehmen nachhaltig gefördert werden. Es galt, interne Sicherheitsstandards zu etablieren, die von allen Mitarbeitenden – vom Management bis zur Produktion – getragen werden.

Auswahlprozess und Kriterien für die SOC-Partnerschaft

Für das Möbelunternehmen war es entscheidend, einen Anbieter zu finden, der nicht nur technische Anforderungen erfüllen konnte, sondern auch als langfristiger, vertrauenswürdiger Partner zur Seite steht.

Wichtige Kriterien bei der Auswahl waren:

✓ **Schnelle Reaktion durch Rund-um-die-Uhr-Schichtbetrieb**

Eine „echte“ 24/7/365-Überwachung sollte sicherstellen, dass Sicherheitsvorfälle und Cyberangriffe standortübergreifend sofort erkannt werden.

✓ **Incident Response**

Zur Entlastung der internen IT-Ressourcen des Kunden mussten Bedrohungen nicht nur erkannt, sondern auch in kürzester Zeit zuverlässig abgewehrt werden.

✓ **Räumliche Nähe**

Das Unternehmen suchte bewusst nach einem Partner, der räumlich nah genug an seinem Hauptsitz war, um im Bedarfsfall schnell vor Ort sein zu können.

✓ **Persönliche Ansprechpartner und Stabilität**

Das Unternehmen legte großen Wert auf eine langfristige Zusammenarbeit mit einem erfahrenen Anbieter und wollte feste technische und beratende Ansprechpartner.

Auch die Kommunikation auf Augenhöhe mit dem SOC-Dienstleister war dem Kunden immens wichtig.

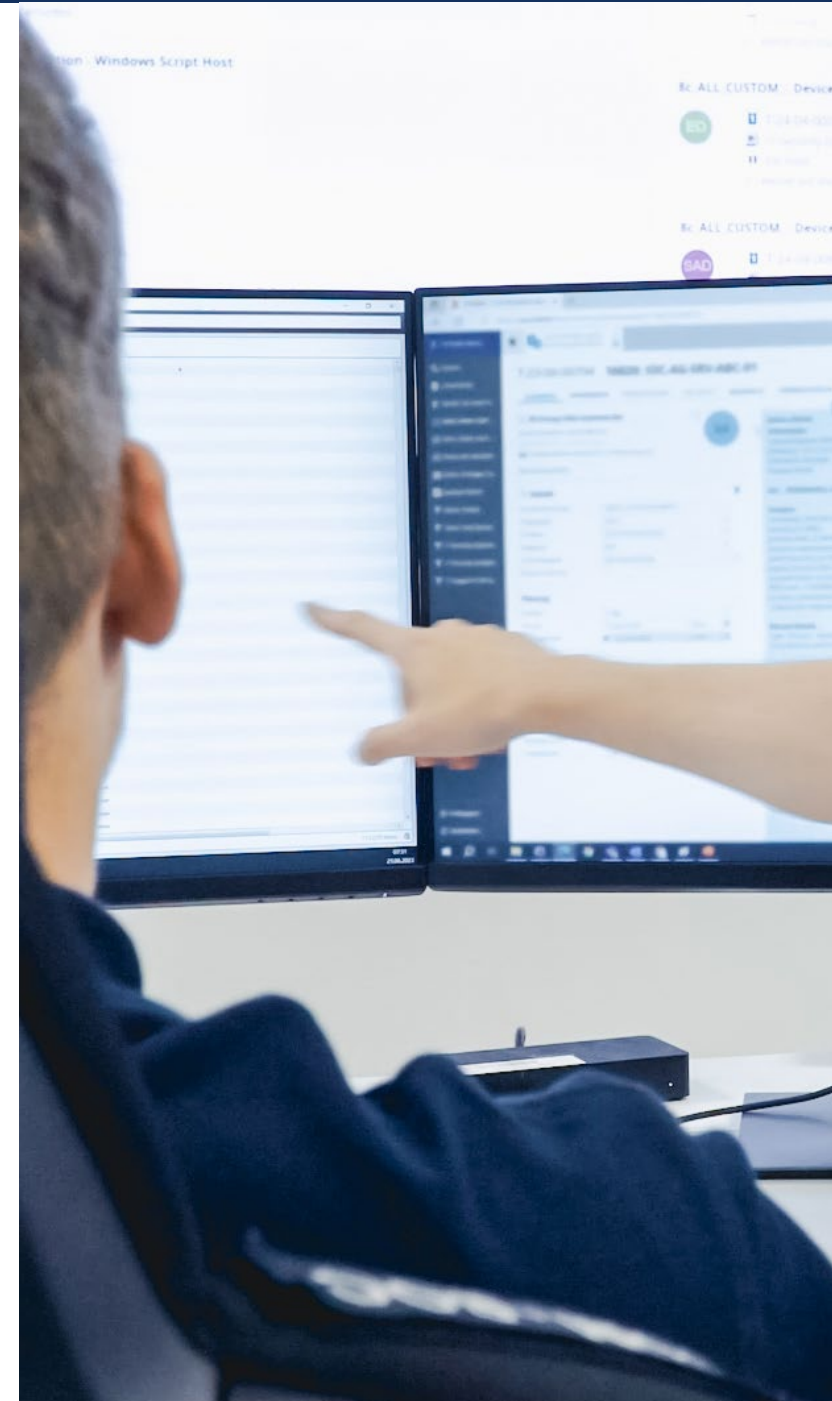
✓ **Transparente Preisgestaltung**

Ein klares, transparentes Preismodell ohne versteckte Kosten oder Überraschungen war Voraussetzung, um die Zusammenarbeit planbar und kalkulierbar zu gestalten.

Inbetriebnahme

Bei der Implementierung des SOC erforderten insbesondere die spezifische Firewall-Konfiguration und die komplexen Anforderungen an die Datensicherheit eine enge Abstimmung. Hinzu kamen die technischen Vorgaben des Rechenzentrums-Dienstleisters des Kunden, die 8com berücksichtigen musste. Dennoch konnte das Vorhaben in einem Zeitraum von sechs Monaten erfolgreich abgeschlossen werden.

Während der Inbetriebnahme arbeiteten das Möbelunternehmen und 8com vertrauensvoll zusammen und entwickelten eine enge Kommunikation, die es ermöglichte, individuelle Sicherheitsbedürfnisse anzusprechen und das System gezielt auf die Infrastruktur des Kunden abzustimmen. Die enge Zusammenarbeit führte zu einem reibungslosen Start des SOC-Betriebs, bei dem nun alle relevanten Datenquellen – von Firewalls und Netzwerkgeräten bis hin zu Windows- und Linux-Servern – zentral überwacht und analysiert werden.





Technische Komponenten und Integration

Aktuell kommen für das Möbelunternehmen im 8com SOC die Technologien SIEM, SOAR und EDR zum Einsatz, die eine umfassende Sicherheitsüberwachung und -analyse ermöglichen. Die wichtigsten Systeme des Unternehmens, einschließlich interner und externer Firewalls, Endgeräte, Windows- und Linux-Server, Hyper-V und Terminal-Server, sind in die Überwachung integriert. Der Datenaustausch zwischen dem Unternehmen und dem SOC erfolgt über Site-to-Site-VPN (IPsec). Dies garantiert eine sichere und verschlüsselte Übertragung der Daten und sorgt dafür, dass das SOC jederzeit auf dem aktuellen Stand ist, um potenzielle Sicherheitsvorfälle – primär über das EDR – in Echtzeit zu erkennen, zu analysieren und einzudämmen. Als nächsten Schritt plant das Unternehmen die Umstellung von EDR auf XDR, um die Erkennung von und Reaktion auf Bedrohungen auszuweiten.

Das 8com SOC führt darüber hinaus regelmäßige Red-Teaming-Übungen und Penetrationstests durch, um die Wirksamkeit der Sicherheitsmaßnahmen zu überprüfen und die bestehenden Alarmregeln kontinuierlich zu optimieren oder neue zusätzliche Alarmregeln zu definieren.

Fazit

Das 8com SOC ermöglicht es der internen IT-Abteilung des Kunden sich wieder auf strategische Aufgaben zu konzentrieren, während das SOC die Überwachung und Analyse von sicherheitsrelevanten Ereignissen sowie die Abwehr von Cyberbedrohungen übernimmt. Ein wesentlicher Vorteil ist auch die verbesserte Sichtbarkeit der Sicherheitslage für das Management, die durch regelmäßige CISO-Reports und Dashboards gewährleistet wird. Diese Berichte erleichtern es dem Kunden, stets aussagefähig zur IT-Sicherheit im Unternehmen zu sein und fundierte Entscheidungen zur Weiterentwicklung der Cybersicherheitsmaßnahmen zu treffen.

Die Beauftragung von 8com hatte positive Auswirkungen auf die Sicherheitskultur im gesamten Unternehmen. Schon durch die Überwachung aller relevanten Systeme und den regelmäßigen Austausch mit 8com stieg das Sicherheitsbewusstsein bei einem Großteil der Mitarbeitenden. Da Meldungen und Dashboards in das tägliche Arbeitsumfeld integriert wurden, sind potenzielle Risiken und Vorfälle für die Verantwortlichen transparent und greifbar. Auch die Managementebene profitierte von einer deutlich verbesserten Einsicht in den Sicherheitsstatus und der Möglichkeit, gezielte Maßnahmen zur Stärkung der IT-Sicherheit zu initiieren. Insgesamt trägt das 8com SOC nun entscheidend zur Absicherung von Prozessen und sensiblen Informationen sowie zur Stärkung der betrieblichen Resilienz bei.



Tipps für andere Unternehmen

Das Möbelunternehmen gibt vor allem folgende Empfehlungen für andere Firmen, die die Beauftragung eines SOC-Dienstleisters in Erwägung ziehen:

✓ SOC vor Ort besichtigen

Eine Überprüfung der Arbeitsweise der SOC-Analysten und der SOC-Räumlichkeiten ist sinnvoll.

✓ Individuelle Alarmregeln und Notfallpläne erstellen

Standards reichen nicht aus, um die kundenspezifischen Prozesse vor Sicherheitsvorfällen umfassend zu schützen. Die individuelle Gestaltung und laufendes Feintuning erhöhen entscheidend die Effizienz der Sicherheitsmaßnahmen.

✓ Notfallübungen durchführen

Tabletop-Übungen oder Rollenspiele helfen, das Notfallmanagement unter nahezu realen Bedingungen zu testen und zu verbessern.

▶ **Haben auch Sie Interesse an einer SOC-Lösung, die Ihre IT-Resilienz auf ein neues Level hebt?**

Nehmen Sie Kontakt zu uns auf! | www.8com.de