Darum sollten Sie in Cybersicherheit investieren

Eine Investition lohnt sich – eine Nicht-Investition wird am Ende teurer

94 %	1,6 Mio €	52 %
der Unternehmen erlebten im letzten Jahr einen Cyberangriff [1]	durchschnittl. Bereinigungskosten nach einem Ransomware-Angriff [2]	können komplexe Cyberbedrohungen nicht selbst bewältigen [1]

1 Cybersecurity-Report 2023: Der Business Impact von Cyberangriffen, Sophos
2 Ransomware-Report 2023, Sophos

Top Risiken

Komplexe Cyberangriffe

Reine Technologie-Lösungen sind mittlerweile machtlos dagegen

Fehlendes Fachwissen

Hochspezialisierte Experten im Bereich Cyberabwehr sind nötig, aber schwer zu finden

Begrenzte Kapazitäten

Zu wenig interne Fachkräfte, nicht möglich, sich 24/7 um Cybersecurity zu kümmern

Warum ist Cybersecurity Verantwortung der Geschäftsführung?

- Geschäftsführungen, Vorstände und Aufsichtsräte sind gesetzlich verpflichtet, die IT-Sicherheit ihres Unternehmens sicherzustellen. Bei Pflichtverletzungen drohen hohe Geldbußen für das Unternehmen und die persönliche Haftung von Entscheidungsträgern und Verantwortlichen (DSGVO, IT-Sicherheitsgesetz 2.0, NIS2-Richtlinie)
- Reputationsschäden durch Cyberangriffe
- Bei Cyberangriff: Umsatzeinbußen; DSGVO: 4 % des Jahresumsatzes droht als Strafe
- Die Budgethoheit liegt bei der Geschäftsführung

Vorteile beim Einsatz des Sophos Cybersecurity Service (Sophos MDR)

- Senkung der Kosten um mindestens das 3-fache gegenüber einem Inhouse Security Operations Center
- Sophos MDR ist kompatibel mit bei Ihnen bereits vorhandenen Cybersecurity-Tools
- Verdopplung der Effizienz der IT-Teams -> Erhöhung der IT-Kapazitäten
- Sie steigern Ihren Cybersecurity ROI und mindern Ihre Risiken
- Sophos ist seit mehr als 37 Jahren am Markt – über 550.000 Kunden weltweit, hohe Expertise, ausgezeichnete Reputation
- Ein Team von 600+ Managed and Response Analysten ist 24/7 an 365 Tagen für Sie im Einsatz und erreichbar
- Bei Sophos sind Sie bestens aufgehoben – wir haben mehr MDR-Kunden als jeder andere Cybersecurity-Anbieter, bereits jetzt weltweit über 15.000

★★★★★

4,8/5
durchschnittliche Bewertung
(Stand: 1. August 2022)

Gartner Peer Insights™

★★★★★

„Top Vendor“
im Grid® 2022 von G2 in der Kategorie MDR-Services für den Midmarket

SOPHOS

Als Geschäftsführer sollten Sie folgende Fragen zum Thema Cybersecurity beantworten können:

- [ ] Wie werden im Rahmen Ihres Cybersicherheits-Programms Industriestandards (NIS2-Richtlinie, ISO, TISAX, KRITIS) und Best Practices umgesetzt?
- [ ] Führt Ihr Unternehmen selbst Lieferanten-Audits durch? Wie stellen Sie sicher, dass Ihre Geschäftspartner in Ihrer Infrastruktur auf dem neuesten Stand der Technik sind?
- [ ] Analysieren Sie mit Ihrer IT-Abteilung Sicherheitsvorfälle und Cyberattacken auf Monats-, Quartals- oder Jahresbasis?
- [ ] Wie viele und welche Arten von Cybersicherheits-Vorfällen werden in einer normalen Woche erkannt?
- [ ] Welche Daten werden wo verarbeitet und gespeichert?
- [ ] Wer hat welche Zugriffsrechte und welche Geschäftsprozesse sind besonders wichtig?
- [ ] Welcher Schaden entsteht Ihnen und Ihrem Unternehmen, wenn die Daten entweder nicht mehr verfügbar sind, manipuliert werden, an Mitbewerber oder die Öffentlichkeit gelangen?
- [ ] Wie umfangreich ist Ihr Incident-Response-Plan und wie oft wird der Plan getestet?

Wenn Sie diese Fragen nicht oder nur unzureichend beantworten können, sollten Sie dringend einen Cybersecurity Service als Unterstützung hinzuziehen.

23-06-20 DE (PC)

SOPHOS