sepago® SOC

DAMIT SIE BEIM THEMA IT-SECURITY KEINE KALTEN FÜSSE BEKOMMEN

sepago®

Wir sind zertifizierter Microsoft- und Citrix-Partner und nehmen am Ziften Activated Partner Program teil. Und wir sind Teilnehmer an der Allianz für Cyber-Sicherheit des BSI.

sepago GmbH
Dillenburger Straße 83 | 51105 Köln
Tel.: +49-221-801939 5 – 0 | Fax: +49-221-801939 5 – 15
www.sepago.de | info@sepago.de

sepago Security Operations Center als Managed Service

Die fortlaufende Vernetzung durch BYOD und IoT gefährdet IT-Systeme zunehmend und macht die Aufgaben der Abwehr komplexer. Zugleich steigt die Anzahl der Angriffe überproportional an. Folglich ist umfassende IT-Sicherheit heute kein stabiler Zustand mehr, sondern ein vielschichtiger Prozess, der permanente Überwachung, gezielte Analyse und schnelle Reaktion erfordert. In unserem **sepago Security Operations Center** führen wir alle notwendigen Teilbereiche des Prozesses zu einem ganzheitlichen Schutzkonzept zusammen, um für Ihre Unternehmens-IT Sicherheit auf einem hohen Niveau zu erreichen:

▪ IT-Security Audits und Workshops | ▪ Managed IT-Security Services | ▪ IT-Security Consulting

---

IT-Sicherheits-Audit für Unternehmen

Im Vorab ermitteln wir, in Anlehnung an die ISO/IEC 27001 Sicherheitsnorm, den Status quo der bestehenden Systeme und der IT-Infrastruktur:

- Bestandaufnahme der vorhandenen IT-Sicherheitstechnologien und –maßnahmen mit Blick auf Netzwerke, Systeme, Applikationen, Sicherheitsrichtlinien und Mitarbeiterschulungen
- Risikobewertung | ▪ Managed IT-Security Services Readiness

Auf Basis der Ergebnisse des Audits erhalten Sie eine Entscheidungsvorlage mit Handlungsempfehlungen für die Härtung Ihrer Systeme und für die Einbindung der von uns empfohlenen Microsoft- und Ziften-Sicherheitstechnologien in Ihre IT-Umgebung.

Managed IT-Security Services

Unsere Managed IT-Security Services gliedern sich in zwei Leistungsbereiche auf:

Monitoring – Sicherheitsrisiken und Cyberangriffe erkennen: Wir überwachen Ihre IT-Infrastruktur dauerhaft mit **automatisierten** Prozessen, basierend auf Windows Defender ATP Technologien und Log Analytics:

- Gezielte Suche nach Schwachstellen in der Struktur und der Konfiguration der Systeme
- Überprüfung der Server auf ungewöhnliche Veränderungen und nicht autorisierte Software
- Analyse des Netzwerkverkehrs und der Netzwerknutzung | ▪ Analyse der Logdaten

Proaktive Bearbeitung der Vorgänge durch unser Spezialistenteam nach einem vorgegebenen Leistungskatalog:

▪ Zusammenführung aller aus dem Monitoring gewonnen Informationen | ▪ Priorisierung | ▪ Kategorisierung | ▪ Stabilisierung
▪ Isolierung/ Quarantäne

IT-Security Consulting

Unsere IT-Security Consulting Angebote teilen sich in zwei Bereiche auf:

Pre-Breach Consulting: Nach einem Sicherheits-Audit oder Security Workshop unterstützen wir Sie gerne mit konkreten Consulting-Leistungen, um Ihre Systeme auf den aktuellen Sicherheitsstandard zu bringen und auf Wunsch in unser Security Operations Center zu überführen. ▪ Härtung der Systeme | ▪ Updates | ▪ Installation und Konfiguration von Windows Defender ATP und Log Analytics

Die Belastbarkeit einer Infrastruktur lässt sich am besten prüfen, indem man sie herausfordert. Wir versetzen uns in die Rolle eines Cyberkriminellen und simulieren einen Angriff auf Ihre Systeme, um Schwachstellen zu identifizieren.
▪ Modulare Penetration Testings | ▪ Advanced Hunting Szenarien

Post-Breach Consulting: Im Schadensfall untersuchen unsere Experten den Ablauf eine Cyberattacke: An welcher Stelle und wie weit ist der Angreifer in die Systeme eingedrungen, welche Schäden hat er verursacht und wie verhindern wir zukünftig ähnlich geartete Angriffe?
▪ Forensik | ▪ Schadensdokumentation | ▪ Schadenseingrenzung | ▪ Bereinigung der Systeme | ▪ DSGVO-konforme Prozessmanagement-Entwicklung | ▪ Sicherheitserhöhende Optimierung Ihrer On-Premises oder hybriden IT-Infrastruktur als Citrix Cloud oder mit Microsoft Azure