baramundi

BARAMUNDI CHECKLISTEN liefern praxisorientierte Step-by-Step Anleitungen für komplexe Fragen und Probleme – kompakt und unkompliziert. Mehr davon finden Sie hier: **www.baramundi.com/checklisten**

IT-Audits: Boosten Sie in 7 Schritten Ihre Infrastruktur

Im schlimmsten Fall lauern Datenlecks und bei Hackern beliebte Schwachstellen in den dunklen Ecken Ihres Netzwerks, während veraltete Technologien und brachliegende Ressourcen das Unternehmen ausbremsen. Ein IT-Audit deckt diese potenziellen Risiken und Mängel auf. Wenn Sie dabei systematisch vorgehen, sichern die Compliance und Effizienz in Ihrem Unternehmen.

Planen

Von Hardware bis Datenmanagement: Identifizieren Sie zu prüfende Bereiche und Systeme. Definieren Sie konkrete Ziele, z.B. die Einhaltung von Compliance zu prüfen.

Dokumentieren

Grundlage ist eine Inventarliste aller Hardware, Software und Netzwerkkomponenten sowie ihrer Konfigurationen. So behalten Sie später einen klaren Überblick über den Fortschritt.

Sicherheit prüfen

Häufig zielen Audits mit Penetrationstests und Schwachstellenanalysen auf bestehende Cybersecurity wie Firewalls und Antivirenprogramme. Prüfen Sie auch die Konfigurationen für Server und Netzwerkkomponenten.

Compliance prüfen

Ob Industriestandards oder Datenschutz, stellen Sie sicher, dass Ihre IT-Infrastruktur den geltenden Vorschriften entspricht. Schütze sie besonders geschäftskritische Daten angemessen, um im Ernstfall den Normalbetrieb schnell wieder aufnehmen zu können.

Leistung optimieren

Analysieren Sie, ob die Systemleistung und Netzwerkinfrastruktur den Anforderungen des Unternehmens entsprechen und ausreichend skalierbar sind.

Aktionsplan erstellen

Dann sollten identifizierte Schwachstellen und Mängel angegangen werden. Ein Aktionsplan legt die Maßnahmen je nach Dringlichkeit fest. Benennen Sie verbindliche Verantwortlichkeiten und Deadlines.

Reporting

Abschließender Schritt ist der Audit-Bericht, der Ergebnisse, Empfehlungen, Prioritäten und mögliche Verbesserungen festhält. Stellen Sie den Bericht den relevanten Stakeholdern zur Verfügung. Er ist die Basis für alle folgenden Maßnahmen.

Kurz gesagt: In regelmäßigen IT-Audits identifizieren Sie Risiken Ihrer Cybersecurity. Ob Inventarisierung, Vulnerability Scanner oder Update Management: Damit Ihr Audit in jedem IT-Teilbereich bestens gelingt, können Sie auf die baramundi Management Suite zählen.