

audius

Durch Schwachstellen in der IT bedrohen Cyberangriffe die Handlungsfähigkeit von Unternehmen immer mehr.

Dadurch wird IT-Sicherheit, Flexibilität und IT-Verfügbarkeit immer wichtiger – doch mit welchem Personal?

audius infrastructure security audit



Mangelnde IT-Sicherheit verursacht Kosten von Ø 3,7 Mio € pro Datenleck.

Wir helfen Ihnen mit unserer langjährigen Erfahrung!



IT-Sicherheit in Ihrem Unternehmen?
Wir schaffen den Überblick.

Wir haben anhand realer Sicherheitsbedrohungen das **audius infrastructure security audit** entwickelt. Mit diesem möchten wir Ihnen dabei helfen, mögliche Schwachstellen frühzeitig erkennen und beseitigen zu können, bevor es zu negativen Folgen kommt.

Das Audit hilft Ihnen, Ihr Unternehmen vor Hackerangriffen, Datenverlust und anderen Bedrohungen zu schützen. Sie sparen dadurch Zeit und Personalkosten.

Die 5 Phasen des Audits:

1. Vorbereitung & Kickoff

- Was wird gemacht?
- Welche Ressourcen werden benötigt
- Zeitplanung

2. Schutzbedarfsanalyse

- Welche Systeme sind vorhanden
- Verfügbarkeit, Schutzziele und Compliance der Systeme

3. Infrastruktur Assessment

- Analyse der Systeme durch audius Frameworks
- Definition von Gegenmaßnahmen

4. Penetrationstests

- Analyse der Systeme durch technische Verifikation
- Erstellung des STAR-Report

5. Report & Abschlusstermin

- Abschlussreport
 - Ist: (Liste der Systeme inkl. Schwachstellen und Risikobewertung)
 - Soll: (Maßnahmenplan, Quickwins, Projektübersicht)
 - Allgemein: (Priorisierung, Projektplan, Wirtschaftlichkeitsbetrachtung)
- Termin zur Ergebnisvorstellung, Q&A, Nächste Schritte



Termin vereinbaren



Weitere Informationen

audius