



Cybersecurity

Fit4Cyber IT-Assessment

Cybersecurity gewinnt in der heutigen vernetzten Gesellschaft immer mehr an Bedeutung. Unternehmen haben mit System- oder Bedienungsfehlern, aber auch mit IT-Verbrechen zu kämpfen.

Durch sich stets ändernde Bedrohungen haben IT-Mitarbeiter alle Hände voll zu tun. Auch die finanziellen Schäden steigen weiter an.

Das **Cybersecurity IT-Assessment** zielt darauf ab, einen Überblick über die gesamte im Unternehmen genutzte Infrastruktur (Hard- und Software) zu geben und potentielle Risiken erkennbar zu machen.

Ganzheitliche Betrachtung: Um die Herausforderungen an Cybersecurity zu verstehen und in der Lage zu sein, die Bedrohungslage einzuschätzen, ist eine ganzheitliche Betrachtung auf Augenhöhe notwendig.

Das Ergebnis ist eine **Cybersecurity Risiko-Tabelle**, die Ihnen einen detaillierten Überblick vorhandener Risiken und deren möglicher Auswirkungen gibt. Vorschläge und Maßnahmen zur Beseitigung des möglichen Risikos sind Bestandteil des „Cybersecurity IT-Assessment“-Berichts, der Ihnen am Ende des Projektes ebenfalls zur Verfügung gestellt wird.

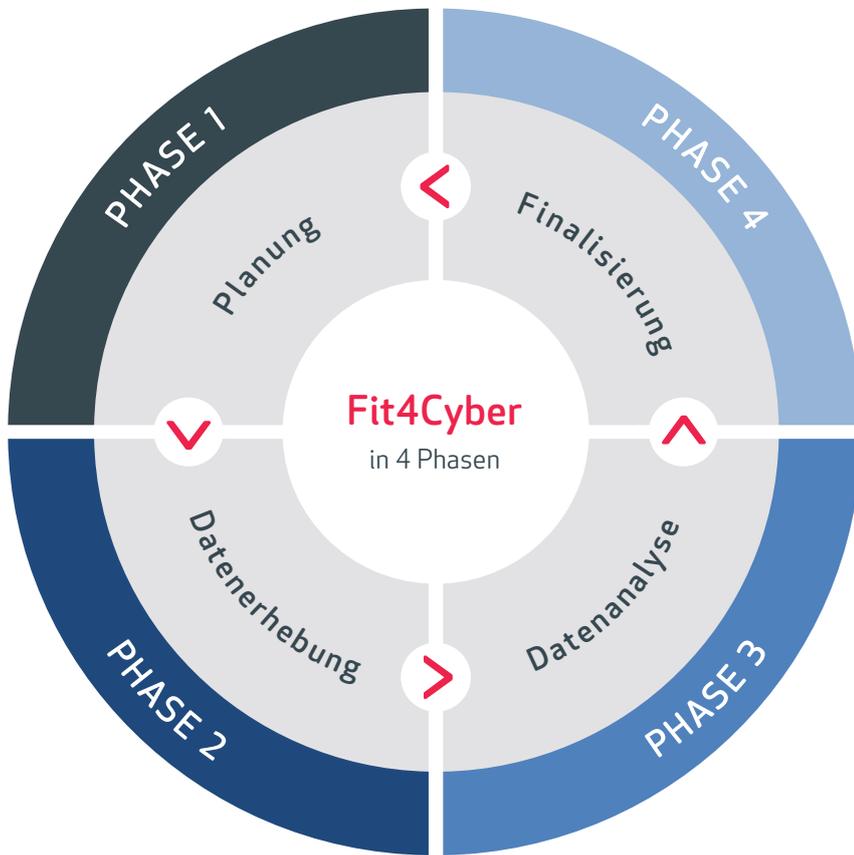
• • • •
 Workshop:
**Fit4Cyber
 IT Assessment***

Ihre Vorteile im Überblick:

- Detaillierter Statuscheck Ihrer Systeme und Prozesse sowie Ermittlung der Infrastruktur-Informationen
- Ermittlung von Netzwerk- und Sicherheitsstrukturen
- Abbildung der Inventur- und Nutzungsdaten
- Management Summary mit Risikobewertung

* Der Workshop umfasst vier Phasen, deren Dauer individuell definiert wird.

Mehr Sicherheit für Ihr Unternehmen.



■ PHASE 1

Planung

- Ermittlung der Infrastruktur-Informationen
- Identifizierung der Projektpläne & Ziele
- Projektplanung
- Festlegung eines Zugangs zur Datenerhebung

■ PHASE 2

Datenerhebung

- Ermittlung von Netzwerk- und Sicherheitsstrukturen
- Darstellung des Software-Inventars sowie Patchlevels
- Abbildung der Inventur- und Nutzungsdaten
- Zusammenführen der Daten für Security Assessment
- Einsatz von Fragebögen & Interviews

■ PHASE 3

Datenanalyse

- Datenvalidierung
- Strategische Ziel-Analyse und Ausrichtung
- Security-Reifegrad

■ PHASE 4

Finalisierung

- Ergebnispräsentation
- Handlungsempfehlung zur Risikominimierung
- IT-Assessment inkl. detaillierter Berichterstellung

Sie möchten mehr über unseren Workshop erfahren?

Dann wenden Sie sich bitte an:

ACP Holding Deutschland GmbH
Otto-Lilienthal-Str. 2
88046 Friedrichshafen

cybersecurity@acp.de
cybersecurity.acp.de



ACP – Ihr Partner vor Ort

ACP ist in Deutschland und Österreich präsent. Gegründet 1993, beschäftigt der IT-Provider mittlerweile über 1.400 Mitarbeiter an mehr als 40 Standorten. ACP bietet als herstellerunabhängiges IT-Systemhaus Consulting, Beschaffung und Integration, Managed Services, Datacenter Services sowie IT-Finanzierung für das gesamte IT-Sortiment für Unternehmen, Behörden und Organisationen jeder Größe.

ACP Gruppe • info@acp.at • info@acp.de
www.acp.at • www.acp.de