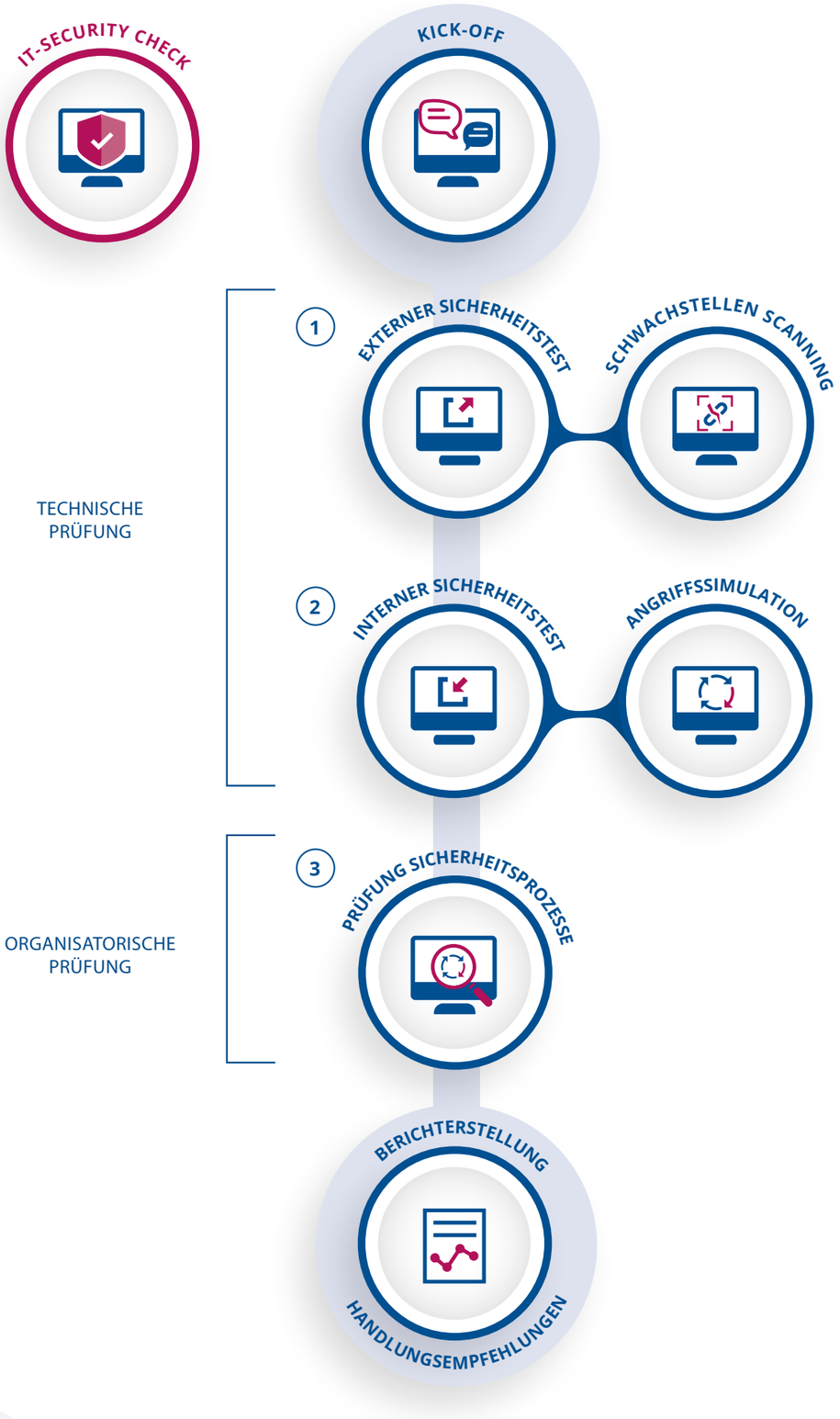
ABLAUF DES IT-SECURITY CHECK



DIE 3 SCHRITTE IM ÜBERBLICK

	A SECURITY CHECK BASIC	B SECURITY CHECK EXTENDED
KICK OFF		
Gemeinsam bereiten wir Ihren IT-Security Check vor. Es werden die Termine vereinbart, die Verantwortlichkeiten festgelegt, die Kernpunkte erläutert sowie alle notwendige Dokumentationen und Berechtigungen bereitgestellt.		
1. EXTERNER SICHERHEITSTEST		
Im ersten Schritt erfolgen Angriffsversuche auf das externe, über das Internet erreichbare Netzwerk in Form eines Schwachstellenscans. Wir scannen betroffene Systeme, evaluieren und protokollieren die jeweiligen Versionen, und identifizieren Schwachstellen, die Angreifer leicht ausnutzen könnten.		
max. 20 aktive Systeme	✓	✓
Oberflächenüberprüfung einer Webapplikation	✓	✓
2. INTERNER SICHERHEITSTEST		
Im zweiten Schritt simulieren wir Angriffsversuche innerhalb des Netzwerks bzw. Systems. Bei dieser Angriffssimulation gehen wir davon aus, dass ein unbefugter Zugriff auf einen Firmencomputer oder auf das Firmennetzwerk hat. Wir überprüfen Benutzerberechtigungen, Netzwerke und Konfigurationen diverse Programme und Sicherheitseinrichtungen auf Schwachstellen. Gefundene Lücken werden ausgenutzt, um die Auswirkungen aufzuzeigen. Tägliche Statusmeetings und ein Abschlussworkshop informieren über diese Sicherheitslücken.		
Sicherheitsprüfung Client	✓	✓
Schwachstellenscan	✗	✓
Prüfung Windows Active Directory	✗	✓
Prüfung 2 Switches/Firewall	✗	✓
Prüfung Security Maßnahmen (A/V, Proxy, NAC, DLP, etc.)	✗	✓
Prüfung WLANs	✗	✓
3. PRÜFUNG SICHERHEITSPROZESSE		
Auf Basis der Ergebnisse der Sicherheitstest eruieren wir alle inneren und äußeren Bedrohungen für dasUnternehmen, untersuchen die bestehende Kontrolleinrichtungen und leiten nötige Maßnahmen zur dauerhaften Implementierung eines hohen Sicherheitsniveaus ab. Als Basis dienen die Top 20 der CIS Critical Security Controls (CSC).		
PRÜFUNG UMGESETZTER SICHERHEITSPROZESSE UND ANGRIFFSVEKTOREN	✓	✓
BERICHTERSTELLUNG		
Die Ergebnisse übermitteln wir Ihnen schriftlich und zeigen auf welche Sicherheitslücken in Ihrem System bestehen, welche Risiken damit einhergehen und wie diese Lücken am besten zu beheben sind. Dieser Endbericht stellt Ihren Sicherheitsstatus dar und gibt Ihnen Handlungsempfehlungen.		
Managementpräsentation und Präsentationsunterlagen (inkl. priorisierten Maßnahmen)	✓	✓
Ergebnisworkshop	✗	✓
schriftlicher Endbericht	✓	✓
Detailgrad	limitiert	hoch