	Stufe 1 - Elementar	Stufe 2 - Proaktiv	Stufe 3 - Resilient
Bedrohungen für persönliche Identitäten	<ul style="list-style-type: none"> > Grundlagentraining zu Social-Engineering-Methoden > Keine Schutzmaßnahmen für persönliche Konten der Mitarbeitenden > Risiko im privaten Bereich hat keine Priorität 	<ul style="list-style-type: none"> > Awareness-Training für Mitarbeitende, doch kein geregelter Schutz für persönliche Identitäten > Mitarbeitende werden zum Schutz privater Konten ermutigt, aber nicht verpflichtet > Schutz von persönlichen Identitäten gilt nur auf Führungs- und Vorstandsebene als wichtig 	<ul style="list-style-type: none"> > Awareness-Programm bezieht Schutz persönlicher Identitäten und Geräte mit ein > Starker Schutz der Identitäten von Führungspersonen und Mitarbeitenden > Laufendes Monitoring auf gestohlene Zugangsdaten
Ungleichgewicht bei Cyberresilienz	<ul style="list-style-type: none"> > Geringe Investitionen in Cybersicherheit > Compliance wird als ärgerliche Verpflichtung betrachtet > Security-Entscheidungen werden reaktiv getroffen 	<ul style="list-style-type: none"> > Schutzmaßnahmen vorhanden, doch Budgets und Support der Führungsebene sind begrenzt > Compliance mit vorgeschriebenen Mindestanforderungen > ISO27k gilt als Orientierungsgrundlage oder wird aufgrund begrenzter Reichweite implementiert > Cyber-Sicherheitsstrategie vorhanden, aber nur kurzfristig > Incident Response Plan nicht getestet oder nicht formell festgehalten 	<ul style="list-style-type: none"> > Sicherheit wird Priorität und entsprechende Ressourcen eingeräumt > Für den Großteil aller wichtigen Systeme ISO27k-zertifiziert > Entwicklung regulatorischer Anforderungen im Austausch mit zuständigen Regierungsbehörden > Aktive Unterstützung der Cyber-Security-Initiativen durch die Führungsebene > Sicherheitsstrategien im Einklang mit Geschäftsanforderungen
Boom der Cybercrime-Branche	<ul style="list-style-type: none"> > Reaktive Haltung gegenüber Cyberbedrohungen > Informationen zu neuesten Angriffstrends aus allgemeinen Quellen bezogen > Keine langfristige Strategie zur Anpassung 	<ul style="list-style-type: none"> > Cybercrime-Trends im Blick, doch die Reaktion beschränkt sich auf direkte Bedrohungen > Sporadisches Sammeln und Weitergeben von Informationen, doch begrenzte Anpassung an neue Angriffstrends > Mitarbeitende werden über Trends informiert, aber nicht regelmäßig dazu geschult 	<ul style="list-style-type: none"> > Sicherheitsstrategie basiert auf personalisierten Threat-Intelligence-Diensten > Stetige Anpassung an neue TTP (Taktiken, Techniken und Prozeduren) der Angreifenden > TTP der Angreifenden zu kennen, gehört zur Unternehmenskultur

Wie steht es um die Sicherheit Ihrer Organisation?

Nutzen Sie unser Assessment für eine individuelle Einschätzung Ihrer Cyber-Resilienz.

Jetzt Cyber-Resilienz testen