Überblick über die IT-Sicherheitsstruktur mit Damovo's Cybersecurity Check

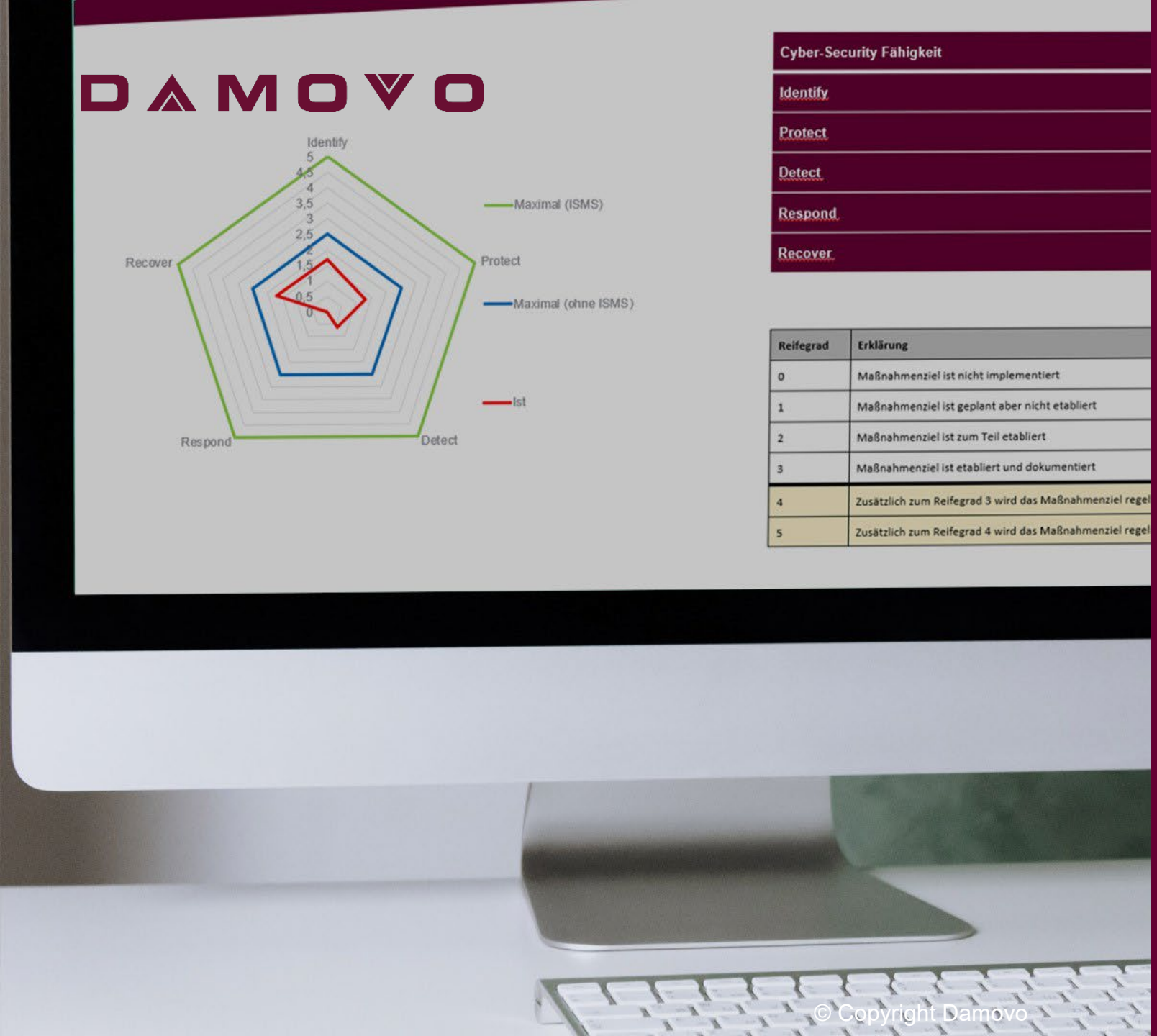
Change Driver

Ein Reise- und Veranstaltungsdienstleister mit Fokussierung auf Kurz- und Bahnreisen wurde aus dem Mutterkonzern ausgegliedert und agiert nun selbstständig.

Alle Belange rund um IT-Sicherheit, sei es konzeptionell oder operativ, wurden bislang vom Mutterkonzern übernommen. Das Unternehmen steht vor der Herausforderung, seine IT-Sicherheit selbständig zu managen und dafür den konzeptionellen Rahmen abzubilden.

Der Verantwortliche für IT und Cybersecurity möchte sich zunächst einen guten Überblick über die bisherige IT-Sicherheitsinfrastruktur verschaffen, um anschließend erforderliche Maßnahmen zu priorisieren und aufzusetzen.

Damovo erhielt mit dem Cybersecurity Check den Zuschlag zur Durchführung.



Damovo Approach

Im Rahmen einer strukturiert geführten Diskussion mit dem Kunden und Damovo Security Experten erfolgte die Bestands-aufnahme der aktuellen IT-Sicherheits-umgebung.

Mittels eines Vulnerability Scan wurden zusätzlich Schwachstellen (von außen in das Unternehmensnetzwerk) geprüft.

Die Ergebnisse wurden anhand eines Reifegrad-Scores, gespiegelt an und untergliedert in den fünf Funktionsebenen des NIST-Frameworks bewertet und übersichtlich aufbereitet.

Der Abschlussbericht beinhaltet zusätzlich Handlungsempfehlungen durchzuführender Maßnahmen, wobei unternehmens-individuelle Aspekte, wie Kritikalität, finanzieller und personeller Rahmen berücksichtigt sind.

Die Ergebnispräsentation erfolgte in einem separaten Termin mit Beteiligung des Projektteams, der IT-Leitung sowie der Geschäftsführung.

Customer Value

DAMOVO

So profitiert der **IT-Leiter**

Bereitstellung einer priorisierten Roadmap zur Verbesserung der IT-Sicherheit.

Klare und belastbare Argumente für die nächste Budgetverhandlung.

Schwachstellen Scan kann auf Anfrage schnell und wiederholt durchgeführt werden, sodass unkompliziert ein Update über offene Ports abrufbar ist.

So profitiert das **Unternehmen**

Die generelle, eigenverantwortliche Verbesserung der IT-Sicherheit im Unternehmen ist initiiert worden.

Risiken und Schwachstellen sind transparent gemacht worden.

Die Minimierung schützt die Daten und Mitarbeitenden des Unternehmens.