

DAMOVO

Overview of the IT Security Structure With Damovo's Cybersecurity Check





Change Driver

A travel and event service provider focussing on short trips and rail travel was spun off from the parent company and now operates independently.

All matters relating to IT security, whether conceptual or operational, were previously handled by the parent company.

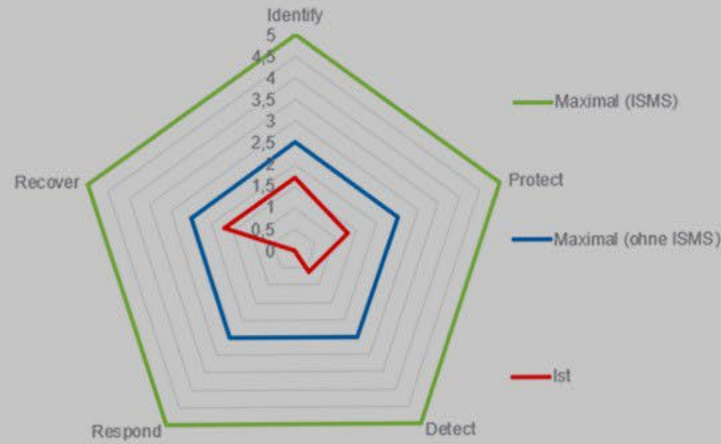
The company faces the challenge of managing its IT security independently and mapping the conceptual framework for this.

The person responsible for IT and cybersecurity first wants to gain a good overview of the existing IT security infrastructure in order to then prioritise and implement the necessary measures.

Damovo was awarded the contract to carry out the cybersecurity check.



DAMOVO



Cyber-Security Fähigkeit

Identify

Protect

Detect

Respond

Recover

| Reifegrad | Erklärung |
|-----------|---------------------------------------------------------|
| 0 | Maßnahmenziel ist nicht implementiert |
| 1 | Maßnahmenziel ist geplant aber nicht etabliert |
| 2 | Maßnahmenziel ist zum Teil etabliert |
| 3 | Maßnahmenziel ist etabliert und dokumentiert |
| 4 | Zusätzlich zum Reifegrad 3 wird das Maßnahmenziel regel |
| 5 | Zusätzlich zum Reifegrad 4 wird das Maßnahmenziel regel |



Damovo Approach

As part of a structured discussion with the customer and Damovo security experts, the current IT security environment was analysed.

Vulnerabilities (from outside into the company network) were also checked by means of a vulnerability scan.

The results were evaluated and clearly presented using a maturity score, mirrored and subdivided into the five functional levels of the NIST framework.

The final report also contains recommendations for measures to be implemented, considering company-specific aspects such as criticality, financial and personnel framework.

The results were presented in a separate meeting with the participation of the project team, IT management and senior management.



How the **IT Manager** benefits

A prioritised roadmap for improving IT security has been provided.

Clear and robust arguments for the next budget negotiation.

Vulnerability scans can be carried out quickly and repeatedly on request so that an update can be easily accessed via open ports.

How the **company** benefits

The general, autonomous improvement of IT security in the company has been initiated.

Risks and vulnerabilities have been made transparent.

Minimisation protects the company's data and employees.