

Design of a vulnerability management



Change Driver

Based on the existing Information Security Management System (ISMS), the security officer of a retail and logistics company deals conceptually with the topic of security.

On the one hand, compliance guidelines require continuous monitoring, risk assessment and, if necessary, updating of systems and applications.

On the other hand, a look at current vulnerability databases shows an increase in weaknesses in systems and applications. Known vulnerabilities can be exploited in a targeted manner, for example with extensive exploits (ready-made attack programmes) and thus even by users with little basic knowledge.

The security officer is therefore focused on the aspect of risk minimisation and must adequately consider vulnerability and patch management as part of cyber hygiene.

However, as these issues cannot be dealt with fully and in a timely manner by the security officer, they require support from an external service provider.



Damovo Approach

As part of a consultancy assignment, Damovo has designed a vulnerability management system that goes far beyond simple patch management.

It is based on a conceptual approach, continuous processes and automation. This is the only way to win the race against attackers.

In addition, vulnerabilities and risk management are linked so that the weakest link in the security chain can be prioritised. Successful attacks can thus be prevented from the outset.

Based on this conceptual approach, Damovo's Vulnerability Management (VM) is used, which is a solution component of Damovo's Security Operation Centre (SOC).



How the **security officer** benefits

The introduction of Damovo's vulnerability management solution has freed up human resources for other tasks compared to the previous manual solution.

The tense relationship with the IT manager, who demands the prompt elimination of existing vulnerabilities, has also been defused.

How the **company** benefits

The vulnerability management solution increases the company's resistance to attacks and thus reduces the cyber risk.

In addition, the requirements of ISO/IEC 27001 and PCI DSS in this area can be fully met by using the solution.