Vulnerability Management Checklist

1. Long-running and unresolved vulnerabilities
   Are there long-standing vulnerabilities in your IT landscape that have not yet been conclusively assessed or resolved?

2. Optimization potential in server processes
   Do you already have optimization potential in the processes of your servers to increase efficiency and security?

3. Completeness of patch management
   Are all relevant patch management processes implemented - or are there gaps that pose an increased risk?

4. Inventory of your IT infrastructure
   Can you guarantee a complete inventory of your systems and applications in order to identify security risks at an early stage?

5. Traceability of history and audits
   How do you ensure the transparent documentation and traceability of all changes and audits in your IT environment?

6. Identification and elimination of process blockers
   Are there internal blockages in your IT processes that, if identified and eliminated, would improve smooth operation?

7. Targeted data exports for service bar
   Are you able to deliver targeted data exports to your external service providers as required?

8. Clearly defined end-to-end processes
   How well are your end-to-end vulnerability management processes documented and monitored - is this sufficient to ensure a holistic approach to security?

9. Measuring success in vulnerability management
   What metrics and processes do you use to continuously measure the success and effectiveness of your vulnerability management?

10. Adaptability to current threats
    How do you ensure that your security and vulnerability management processes are always adapted to current threats and technological developments?

Have you not been able to check off all the points? Then we are here for you - get in touch with us!

Arvato Systems| Christine Niehage & Carolina Loew| E-Mail: cybercare@arvato-systems.de |arvato-systems.com