DTS

CYBERSECURITY STRATEGY WORKSHOP

> “By failing to prepare, you are preparing to fail.”
>
> Benjamin Franklin

Today, cybersecurity requires far more than a firewall and an antivirus program. Companies must systematically analyze where the weak points are, which systems are particularly worth protecting and which individual security level is appropriate.

In today’s digital age, an effective cybersecurity strategy is essential for companies. The increasing reliance on digital technologies, cloud services and connected devices has significantly increased the threat landscape. Against this backdrop, it is crucial not to view cybersecurity in isolation, but to integrate it as an integral part of the business strategy and proactively incorporate it into corporate decisions.

Our unique Cybersecurity Strategy Workshop takes your security strategy to a new level - innovative and absolutely future-oriented. An experienced DTS Cybersecurity Coach analyzes the existing approaches of the security strategy and identifies the most important data, assets, applications and services that need to be protected. Based on this, optimized workflows are developed with the help of proven principles such as the Zero Trust model and the best practices of Critical Security Controls. This also takes into account the necessary implementation of compliance guidelines such as NIS2.

The DTS approach aims to develop a fundamental understanding of the practices and processes necessary to minimize cybersecurity risks. A sustainable security strategy strengthens a company not only against current threats, but also against future threats.

Are you looking for a long-term partner for the development of a continuous cybersecurity strategy? We can support you here too! As a “Trusted Advisor”, DTS offers a regular service with ongoing reviews for the joint design of a resilient security strategy. Invest in the security of your company!

TOPICS OF THE WORKSHOP

- Prioritization of current security challenges
- Understand & apply Zero Trust basic principles
- Recommendations for the practical implementation of Critical Security Controls
- Identify the three most important core data, assets, applications and services in the company
- Develop efficient processes to secure the three defined resources

AIM OF THE WORKSHOP: To develop a basic understanding of a resilient cybersecurity strategy as well as presentation and reporting of the optimized processes

DTS Systeme GmbH
+49 5221 1013-000

DTS Systeme Münster GmbH
+49 251 6060-0

dts.de
info@dts.de