ASSUME BREACH ASSESSMENT

In our 3-day Assume Breach Assessment, DTS security experts carry out real attacks on your IT environment. The result is the answer to the question: How vulnerable are your business capabilities and the entire organization?

AT A GLANCE

- Cost-effective price for the ideal introduction to the question: "How secure is my company?"
- Determination of the resilience and current status of your IT security
- Verification and identification of the attack surface and specific IT vulnerabilities
- Status quo regarding the security of your internal network
- Realistic attacks by offensive security experts?
- In-depth support and consideration of the customer-specific context
- Focus: Active Directory
- Long-term and sustainable recommendations for action
- Preventive and proactive measures
- DTS as a cyber security specialist and strong IT partner for "everything from a single source"

UNIQUE QUALITY. ATTRACTIVE PRICE. FULL INSIGHT INTO YOUR RISK!

With our exclusive service, we offer you the opportunity to identify real risks in your IT landscape. Our offensive cyber security experts evaluate attack paths and their chances of success, security deficits, and the ability to protect against malware. The service is not a "normal" assessment or a full penetration test of the entire internal network. Instead, it focuses on a reduced scope to show you the basic cyber resilience of your company.

METHODOLOGY

Our specialists assume the role of hackers. We attempt to compromise systems, gain access rights, and deploy ransomware. We gather initial information through vulnerability analysis. We also examine your internal network. Post-exploitation activities are then carried out, e.g., to expand rights. The linchpin is Active Directory as the center for administrative activities.

ASSUME BREACH ASSESSMENT

- Onboarding: Registration on the DTS reporting platform & relevant hardware is prepared and made available
- Kick-off meeting: Discussion of the detailed technical project process and definition of customer-specific assessment goals & Active Directory domains to be included in the scope
- Performance of the assessment & all findings are documented on the DTS reporting platform
- Final meeting: Explanation of the results and presentation of an overview of possible long-term measures to improve your IT security and short-term recommendations for action to eliminate acute vulnerabilities Optional: You can also edit your results independently on the platform and request retests