DACHERSYSTEMS
value-added-IT

WHiTEPAPER
CYBERSECURiTY

Allianz für Cyber-Sicherheit
Teilnehmer

We detect hidden system vulnerabilities before hackers do!

Facts, background and costs

We do not need to explain that a real cyber threat exists and will unfortunately continue to increase in the future. The German Federal Office for Information Security (BSI) assesses the threat situation for IT security in Germany as tense to critical[1]. The damage caused by system failures, as well as the potential damage to the company's image due to the leakage of sensitive customer data, is immense - for example, if personal data as well as information or booking and payment histories are affected and offered on the darknet after an attack. In the focus of this white paper, we want to show on two pages how to position your company securely and protect it from such attacks. First of all, all vulnerabilities must be found. To do this, we pursue various approaches. But let's start at the beginning.

FOUR POiNTS
YOU NEED TO KNOW iN ADVANCE

LEGAL ASPECTS GDPR:

The General Data Protection Regulation (GDPR) takes a risk-oriented approach to a company's technical and organizational measures. Typical attack methods are:


Identity theft and Data misuse


Phising


Intruder attack


Cyber extortion

An implementation of IT security measures in accordance with the GDPR includes the need to update one's own IT and information security. Penetration testing enables the rapid detection and elimination of IT and security vulnerabilities that could result in a loss of data. But what exactly are penetration tests? In a penetration test (pentest), IT systems as well as networks are subjected to a comprehensive audit designed to determine their susceptibility to attack. A pentest uses methods and techniques that are used by real attackers or hackers.

[1] https://www.bsi.bund.de/DE/Service-Navi/Presse/Pressemitteilungen/Presse2021/211021_Lagebericht.html

THE THREE PHASES OF OUR PENETRATION TEST:

PHASE I

- Information gathering
- Research in publicly available sources for DNS names, RIPE entries, blacklists, metadata analysis, social media.

GOAL: What is your company's technical external exposure

PHASE II

- Identify security vulnerabilities
- Identify vulnerabilities through automated scanning

GOAL: Identify detailed security vulnerabilities via "open" ports, unprotected applications, and known vulnerabilities and misconfigurations of your IT systems.

PHASE III:

- Analyze and fix the security vulnerabilities
- Review and attempt to exploit the found vulnerabilities for malware.auszunutzen.

GOAL: Risk assessment of the potential damage as well as our recommendation on how to fix the possible security holes

PROCEDURE OF A PENETRATION TEST:

In a preliminary discussion between the company IT security officer and our project manager, the objectives and the subject of the security test will be defined. It is imperative that the objectives, action limits and resources involved are coordinated in advance. In our tests, we always keep an eye on importance to system-protecting and silent execution. Your employees or customers should not notice anything.

We usually plan our activities based on the following facts:

- Number of systems to be tested
- Type of systems to be checked
- Number of verification scenarios
- Type and scope of the findings documentation

As a time window we plan between two and four weeks.

Free 15 min Call with one of our security experts.

COSTS OF A PENETRATION TEST

The costs mainly depend on the following two factors mainly:
- Company size (employees, server systems, onPrem or cloud-based)
- Security testing method used

White box, black box, as well as grey box audits have established themselves as the most common test procedures. For better differentiation, always assume the knowledge profile of an attacker. A grey box audit is a combination of black box and white box audits. We recommend to start with an IT vulnerability analysis which, scans the inside infrastructure first and based on the respective results, either a white-, black- or grey-box audit will be carried out afterwards.

BASIC AUDIT

Standard vulnerability scan on defined number of IP addresses. Creation of a result report on all vulnerabilities found incl. prioitization of potential threats.

Costs for companies with < 250 employees and < 9 systems approx. **3.900,- €**

WHITE BOX AUDIT

Within the scope of a white box audit, all relevant data is available to our project manager prior to the start of the test. IT security audit of pre-defined systems for currently existing security gaps.

Costs for companies with < 250 employees and < 9 systems approx. **9.800,- €**

BLACK BOX AUDIT

Within the scope of a black box audit, hardly any relevant data is available to our project manager before the start of the test. IT security check of predefined IP addresses for currently existing security gaps.

Costs for companies with < 250 employees and < 9 systems approx. **16.900,- €**

If you have any questions, our team of experts in Berlin would be happy to answer them. Dacher Systems GmbH was founded in 2005 by the actual Managing Director, Tiberius Dacher and since the beginning we have been focused on all kinds of security topics, cybersecurity, digitalization and blockchain. We guarantee that we will find the best strategy for your company based on our proven IT experience. Dacher Systems GmbH is member of Allianz für Cyber-Sicherheit (ACS).

Trust us and initiate contact today.

Seeburger Str 25c
13581 Berlin, Germany

+49 (0)30 39 800 910

td@dacher-systems.de