IT-SECURITY

PENTESTS

On the way to an efficient Cyber Resilience

Why penetration testing?
Pentests examine your IT infrastructure and systems in a comprehensive manner. This way you can determine how exploitable your infrastructure is. A pentest applies methods and techniques which are also used by attackers or hackers in order to detect weaknesses.

syracom
business efficiency engineering

DO YOU OPERATE YOUR OWN IT INFRASTRUCTURE?

A complex task that requires permanent maintenance.

New vulnerabilities of operating systems and applications are identified almost daily. Even one unresolved security gap can endanger the availability and integrity of an entire corporate network. There are various examples of the devastating attack effects, demonstrated by cases such as the WannaCry 2017 security incident and the Ransomware Ragnarok case.

The assets of your IT infrastructure are ex-tremely worthwhile targets for hackers. They often have large financial resources, know-how and the necessary time to identify the weaknesses of your network. Many attacks even occur from within the company network. Protecting the network boundaries alone does not go far enough.

Common vulnerability scanners do not offer comprehensive protection due to their focus on public vulnerabilities of operating systems and applications: Weak passwords or deficiencies in the configuration are rarely detected. In many scenarios, they also provide many irrelevant results or false positives.

OUR RANGE OF SERVICES AND APPROACH

HIGHLY AUTOMATED PENTESTS

REALITY CHECK

RESULTS REPORT

CLOSE GAPS

Classical penetration tests map the approach of real attackers and identify real, exploitable vulnerabilities in infrastructures (without false positives). However, they are often very expen-sive. Their approach, as well as their results, strongly depend on the skills and perspective of the pentesters. Due to these facts, classical pentests are neither reproducible nor measura-ble.

Highly automated pentests offered by syracom, on the other hand, solve these issues. Fur-ther, they are much easier and faster to implement. These pentests are carried out in an agent-free manner with the PenTera platform from our partner Pcysys. No software installa-tion is required on your devices.

Our IT security team assumes the role of the hacker in the pentest. With the help of PenTera, we carry out a high number of attacks that would manually take several weeks. Results are available in just one or two days. Your systems are attacked in a targeted, measurable and reproducible manner.

syracom acts not only as an attacker, but also as an advisor and helps to interpret the results during and after the penetration test.

Our IT security team assumes the role of the hacker in the pentest. With the help of PenTera, we carry out a high number of attacks that would manually take several weeks. Results are available in just one or two days. Your systems are attacked in a targeted, measurable and reproducible manner.

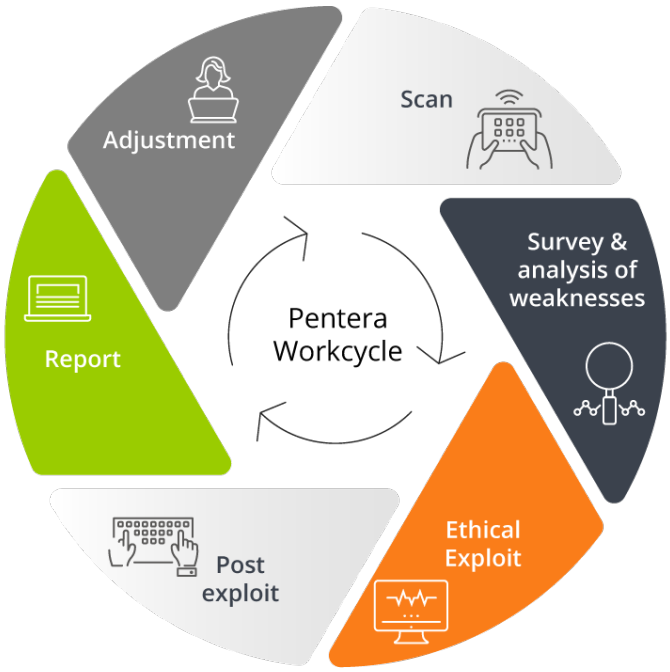
syracom acts not only as an attacker, but also as an advisor and helps to interpret the results during and after the penetration test.

PENETRATION TESTING PROCEDURE

We are using current hacking techniques to carry out ethical exploits based on the we-aknesses of your infrastructure. Our process works for any industry as well as any company size. Further it is fully repro-ducible in real time due to automated exe-cution. Simulta-neously, the involved par-ties always keep both overview and con-trol!

Following our detailed penetration testing procedure, the customer receives compre-hen-sive results and a corresponding man-agement report as shown in the report be-low.

Based on the hereby identified gaps, we independently provide you with guidance for implement-ing the curse of actions.



TOP4ACTIONS

9,8

The host is vulnerable to BlueKeep (CVE-2019-0708)

It is recommended to patch the host for BlueKeep (CVE-2019-0708). Please click on the following link for more information: https://technet.microsoft.com/library/security/CVE-2019-0708

9,3

The host is vulnerable to MS17-010

It is recommended to patch the host for this vulnerability. Please click on the following link for more information: https://technet.microsoft.com/library/security/MS17-010

8,8

Anti Virus did not block malicious user data

Strengthen your anti-virus policies and monitor suspicious behavior on the network.

7,8

Decrypted Chrome Passwords

While scanning web browsers for information, an attacker can find stored credentials and use them to misappropriate the organization's internal and external assets.

HOLISTIC IT SECURITY APPROACH

Our holistic approach provides a well-founded assessment of your IT infrastructure's cyber secu-rity resilience – continuously. An exemplary building block of this approach is the following pentest use case called reality check: A reality-based pentest scenario that helps the customer to understand attacks, their im-pact as well as the reaction within the company e.g. people, processes, SOC or SIEM. In addition, we offer you audits to validate your identity and access management systems and advise you on topics such as multi-factor authentication. All these methods are tailored to both, the com-pany and the specific situation. Moreover, we are able to perform pentests completely remote and implement solution modules with minimal physical presence.

brandeins /thema 2022 Heft 22 Beste Unternehmens-berater

25
Years in the service of customers

210
Employees

30
Turnover in millions of euros

You are welcome to contact us

We are happy to provide you with an individual proof of value and an offer tailored to your company's individual needs. We are looking forward to your request!

YOUR CONTACT

Frank Hoffmann
Head of IT Security

+49 6122 9176 0
frank.hoffmann@syracom.de

syracom AG
Otto-von-Guericke-Ring 15
65205 Wiesbaden (Germany)
+49 61 22 9176 0

syracom.de