IT Security Check SME

Results Report: MegaCorp

24.06.2022

ALTERSOLUTIONS
GERMANY

1 Project overview

1.1 Description

The "IT Security Check SME" is a product developed by Alter Solutions Germany that is specifically tailored to the needs of small and medium-sized enterprises. Within a few days and at low cost, companies receive a comprehensive and individualized overview of the state of their IT security. The security of externally accessible servers and services, the security of the internal network, and the maturity of the IT security organization are all taken into account. Unlike many comparable offerings, the "IT Security Check SME" is not based exclusively on automated scans and the completion of questionnaires, but is carried out manually by experienced penetration testers and in personal discussions with experts in information security management. As a result, companies receive concrete recommendations for action tailored specifically to their needs, which can be used to sustainably improve the state of IT security.

1.2 Methodology

The procedure outlined below was used in this project:

- Security testing of externally accessible services and websites using automated tools and manual checks (1 day).
    - Check for known vulnerabilities and outdated software versions
    - Testing of login functions and session management
    - Checking for injection attacks
    - Checking of access control mechanisms and desired file accesses
    - Testing of password security of administration accesses
- Manual security test of the internal network with support of automated tools (2 days)
    - Check for known vulnerabilities and outdated software versions
    - Checking the configuration of the Windows domain network
    - Checking for security-relevant configuration errors
    - Examination of the possibility of an extension of rights in the network
- Examination of the IT security organization in a personal meeting with management, IT management, information security officer or with an employee in a comparable position (1 day)

1.3 Scope

- External services and websites
  - https://www.megacorp.de
- Internal network
  - IP address range 172.0.0.0/24

2 Managementsummary

The overall state of IT security at MegaCorp is considered critical. Both in external, as well as internal IT systems, several critical vulnerabilities were found. In addition numerous important measures are missing from the IT security organization or have been inadequately
implemented. We see an urgent need for action to prevent a critical IT security incident.

2.1 Recommendations

We recommend implementing the following measures immediately:

- Change the password for remote administration access.
- Updating the Microsoft Exchange Server

In addition, other measures should also be implemented in perspective:

- Carry out regular and automated vulnerability scans (e.g., with the software Nessus) to identify critical security vulnerabilities in internal server systems.
- Establish a patch management system to ensure that identified security gaps are promptly remedied in a timely manner
- Introduction of a backup strategy

2.1 Summary of the identified vulnerabilities

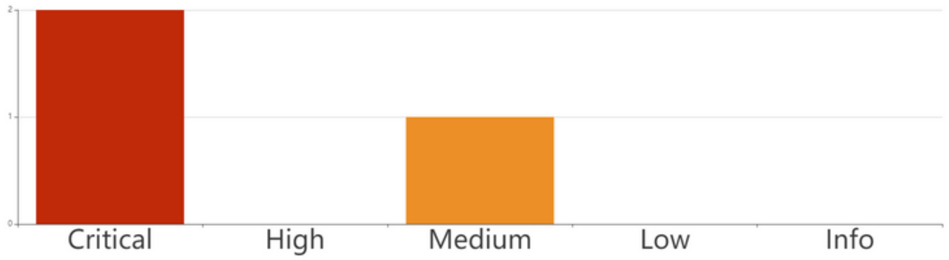


Figure 1: Overview of the severity of the identified vulnerabilities

# 1 Critical Insufficient password protection for remote maintenance access

# 2 Critical Vulnerable Software Version of Microsoft Exchange Server (especially Outlook Web Access)

# 3 Medium No Backup concept available

3 Maturity level of the IT security organization

As part of the IT security analysis, the maturity level of your IT security organization is assessed in terms of the following criteria:

- Asset Management:
- ...

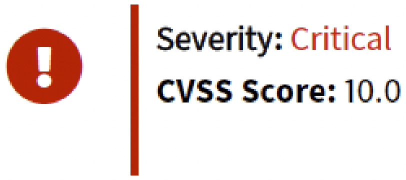
The evaluation is carried out according to four levels:

- Level 0: No measures have been implemented yet
- Level 1: The first suitable measures have been implemented or are about to be implemented.
- Level 2: The most important measures have already been implemented
- Level 3: All relevant measures have been implemented

Category	Status of Implementation	Recommendations
Asset Management	L1	
Risk Management	L1	
Policies	L1	
Training and Awareness Measures	L2	
Backup Strategy	L0	
Log Management	L1	
Permissions	L1	
Configuration and Patch Management	L1	
Mobile Device Management	L1	
Supplementary Security Measures	L2	

4 Details of the Vulnerabilities found

4.1 Inadequate Password Protection for Remote Maintenance Access



Severity: Critical

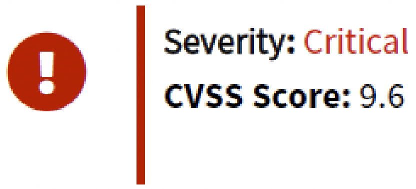
CVSS Score: 10.0

Description
For remote maintenance purposes MegaCorp operates the VNC server "tigerVNC". For the user "Administrator"" a password was assigned which corresponds to the company name.

Impact
By exploiting this vulnerability, attackers can gain administrative access to the internal company network. This could lead to the theft of sensitive data or the sabotage of IT systems. sabotaged - for example, by installing an encryption Trojan.

Recommendation
A strong password (at least 16 characters, preferably with special characters, upper and lower case letters and numbers) should be used. If possible, two-factor authentication should also be factor authentication should be activated.

4.2 Vulnerable Software Version of Microsoft Exchange Server (especially Outlook Web Access)



Severity: Critical

CVSS Score: 9.6

Description
The version of the operated Exchange Server is outdated and contains a severe security vulnerability (CVE-2021-26427). This can be exploited via the Outlook Web Access service running on the Internet.

Impact
The vulnerability in Microsoft Exchange Server has been actively exploited by criminals for automated installation of encryption Trojans for some time. The threat to the internal IT infrastructure and thus to the continued existence of the company is therefore very high. With the exploitation of the vulnerability is to be expected at any time.

Recommendation
The Microsoft Exchange Server should be updated immediately.

References
https://nvd.nist.gov/vuln/detail/CVE-2021-26427

4.3 No Backup Concept available

Severity: Medium

Description
There is currently no backup concept in the company. Although local backups of sensitive files are occasionally made manually, this is not automated and does not affect server systems.

Impact
In case of a major data loss (due to technical reasons or a successful attack), there is currently no possibility to restore lost data. Depending on the extent of the data loss this can have existence-threatening effects.

Recommendation
A company-wide backup concept should be introduced and implemented. In particular and sensitive data should be regularly backed up on a backup system that is as isolated as possible. backup system. The recovery of this data should be tested regularly.