# IT Security Check KMU

## Ergebnisbericht: MegaCorp

22-04-2022

ALTERSOLUTIONS DEUTSCHLAND

# Inhaltsverzeichnis

# 1 Projektüberblick

## 1.1 Beschreibung

Der „IT Security Check KMU“ ist ein von Alter Solutions Deutschland entwickeltes Produkt, das speziell auf die Bedürfnisse von kleinen und mittleren Unternehmen zugeschnitten ist. Innerhalb von wenigen Tagen und zu geringen Kosten, erhalten Unternehmen einen umfassenden und individuellen Überblick über den Stand ihrer IT-Sicherheit. Dabei wird sowohl die Sicherheit von extern erreichbaren Servern und Diensten, die Sicherheit des internen Netzwerks, als auch der Reifegrad der IT-Sicherheitsorganisation berücksichtigt. Anders als viele vergleichbare Angebote, basiert der „IT Security Check KMU“ nicht ausschließlich auf automatisierten Scans und dem Ausfüllen von Fragebögen, sondern wird manuell von erfahrenen Penetration Testern und im persönlichen Gespräch mit Experten im Informationssicherheitsmanagement durchgeführt. Als Ergebnis erhalten Unternehmen konkrete und speziell auf ihre Bedürfnisse zugeschnittene Handlungsempfehlungen, mit denen der Stand der IT-Sicherheit nachhaltig verbessert werden kann.

## 1.2 Methodik

Im Rahmen dieses Projektes wurde die im Folgenden dargestellte Vorgehensweise angewendet:

- Sicherheitstest der extern erreichbaren Dienste und Webseiten unter Anwendung von automatisierten Werkzeugen und manuellen Prüfungen (1 Tag)
  - Prüfung auf bekannte Schwachstellen und veraltete Softwareversionen
  - Prüfung von Login-Funktionen und Session-Management
  - Prüfung auf Injection-Angriffe
  - Prüfung von Zugriffskontrollmechanismen und gewünschten Dateizugriffen
  - Prüfung des Passwortsicherheit von Administrationszugängen
- Manueller Sicherheitstest des internen Netzwerks mit Unterstützung von automatisierten Werkzeugen (2 Tage)
  - Prüfung auf bekannte Schwachstellen und veraltete Softwareversionen
  - Prüfung der Konfiguration des Windows-Domänennetzwerks
  - Prüfung auf sicherheitsrelevante Konfigurationsfehler
  - Prüfung der Möglichkeit einer Rechteausweitung im Netzwerk
- Prüfung der IT-Sicherheitsorganisation im persönlichen Gespräch mit Geschäftsführung, IT-Leitung, Informationssicherheitsbeauftragtem oder mit einem Mitarbeitenden in vergleichbarer Position (1 Tag)

## 1.3 Scope

- Externe Dienste und Webseiten
  - https://www.megacorp.de
- Internes Netzwerk
  - IP-Adresbereich 172.0.0.0/24

# 2 Managementzusammenfassung

Die Stand der IT-Sicherheit bei MegaCorp ist insgesamt als kritisch anzusehen. Sowohl in externen, als auch in internen IT-Systemen wurden mehrere kritische Schwachstellen gefunden. Darüber hinaus fehlen zahlreiche wichtige Maßnahmen in der IT-Sicherheitsorganisation oder sind unzureichend umgesetzt. Wir sehen dringenden Handlungsbedarf, um einen kritischen IT-Sicherheitsvorfall zu vermeiden.

## 2.1 Empfehlungen

Wir empfehlen die folgenden Maßnahmen unverzüglich umzusetzen:

- Ändern des Passworts für den Fernadministrationszugang
- Aktualisieren von Microsoft Exchange Server

Darüber hinaus sollten perspektivisch auch noch weitere Maßnahmen umgesetzt werden:

- Durchführen von regelmäßigen und automatisierten Schwachstellenscans (bspw. mit der Software Nessus) zur Identifikation von kritischen Sicherheitslücken in internen Serversystemen
- Etablieren eines Patchmanagements, mit dem sichergestellt werden kann, dass identifizierte Sicherheitslücken zeitnah behoben werden
- Einführung einer Backup-Strategie

## 2.2 Zusammenfassung der identifizierten Schwachstellen

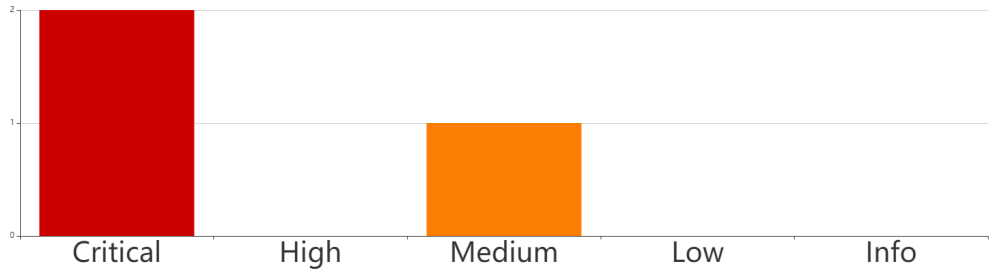


**Abbildung 1:** Übersicht über die Schwere der identifizierten Schwachstellen

**# 1 Critical** Unzureichender Passwortschutz für den Fernwartungszugang

**# 2 Critical** Verwundbare Softwareversion von Microsoft Exchange Server (insbesondere Outlook Web Access)

**# 3 Medium** Kein Backup-Konzept vorhanden

# 3 Reifegrad der IT-Sicherheitsorganisation

Im Rahmen der IT-Sicherheitsanalyse wird der Reifegrad Ihrer IT-Sicherheitsorganisation hinsichtlich der folgenden Kriterien bewertet:

- Asset Management:
- …

Die Bewertung erfolgt dabei jeweils nach vier Stufen:

- Level 0: Bisher wurden noch keine Maßnahmen umgesetzt
- Level 1: Erste geeignete Maßnahmen wurden umgesetzt oder befinden sich kurz vor der Umsetzung
- Level 2: Die wichtigsten Maßnahmen wurden bereits umgesetzt
- Level 3: Alle relevanten Maßnahmen wurden umgesetzt

| Kategorie | Umsetzungsstand | Empfehlungen |
|---|---|---|
| Asset Management | L1 | |
| Risikomanagement | L1 | |
| Richtlinien | L1 | |
| Schulungen und Awareness-Maßnahmen | L2 | |
| Backup-Strategie | L0 | |
| Log Management | L1 | |
| Zugriffsrechte | L1 | |
| Konfigurations- und Patchmanagement | L1 | |
| Verwaltung mobiler Geräte | L1 | |
| Ergänzende Sicherheitsmaßnahmen | L2 | |

# 4 Details der gefundenen Schwachstellen

## 4.1 Unzureichender Passwortschutz für den Fernwartungszugang

**Schwere:** Critical
**CVSS Score:** 10.0

### Beschreibung

Für Fernwartungszwecke betreibt MegaCorp den VNC-Server „tigerVNC“. Für den Benutzer „Administrator“ wurde ein Passwort vergeben, das dem Firmennamen entspricht.

### Auswirkung

Durch Ausnutzen dieser Sicherheitslücke können sich Angreifer Administrationszugang zum internen Firmennetzerk verschaffen. Dadurch können sensible Daten gestohlen, oder IT-Systeme sabotiert werden – beispielsweise durch die Installation eines Verschlüsselungstrojaners.

### Empfehlung

Für den Zugang sollte ein starkes Passwort (mindestens 16 Zeichen, bestenfalls mit Sonderzeichen, Groß- und Kleinbuchstaben und Zahlen) verwendet werden. Sofern möglich, sollte zusätzlich Zwei-Faktor-Authentifizierung aktiviert werden.

## 4.2 Verwundbare Softwareversion von Microsoft Exchange Server (insbesondere Outlook Web Access)

**Schwere:** Critical
**CVSS Score:** 9.6

### Beschreibung

Die Version des betriebenen Exchange Servers ist veraltet und beinhaltet eine schwere Sicherheitslücke (CVE-2021-26427). Diese kann über den im Internet betriebenen Outlook Web Access Dienst ausgenutzt werden.

### Auswirkung

Die Sicherheitslücke in Microsoft Exchange Server wird seit einiger Zeit von Kriminellen aktiv zur automatisierten Installation von Verschlüsselungstrojanern ausgenutzt. Die Bedrohung für die interne IT-Infrastruktur und damit für den Fortbestand des Unternehmens ist daher sehr hoch. Mit der Ausnutzung der Sicherheitslücke ist jederzeit zu rechnen.

### Empfehlung

Der Microsoft Exchange Server sollte unverzüglich aktualisiert werden.

### Referenzen

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

## 4.3 Kein Backup-Konzept vorhanden

**Schwere:** Medium

### Beschreibung

Im Unternehmen ist aktuell kein Backup-Konzept vorhanden. Zwar werden vereinzelt manuell lokale Sicherungen von sensiblen Dateien gemacht, das erfolgt jedoch nicht automatisiert und betrifft auch keine Server-Systeme.

### Auswirkung

Sollte es zu einem größeren Datenverlust bekommen (technisch bedingt oder durch einen erfolgreichen Angriff), gibt es aktuell keine Möglichkeit verlorene Daten wiederherzustellen. Je nach Ausmaß des Datenverlusts kann das existenzbedrohende Auswirkungen haben.

### Empfehlung

Es sollte ein unternehmensweites Backup-Konzept eingeführt und umgesetzt werden. Insbesondere sollten unternehmenskritische und sensible Daten regelmäßig auf einem weitestgehend isolierten Backup-System gesichert werden. Die Wiederherstellung dieser Daten sollte regelmäßig getestet werden.