NETZ EXPERTEN

Management-Zusammenfassung

Zusammenfassung der Penetrationstests

Erstellt von NetzExperten Unternehmensberatung GmbH & Co.KG

BEISPIELAUSZUG EINES PENTEST-REPORTS – ALLE VERTRAULICHEN INFORMATIONEN WURDEN ENTFERNT.

NETZ EXPERTEN

Inhaltsverzeichnis

Hintergrund

Zwischen [redacted] und dem [redacted] wurde von NetzExperten Unternehmensberatung GmbH & Co.KG ein interner Netzwerk-Penetrationstest für [redacted] durchgeführt. Für die Durchführung der Penetrationstests und die anschließenden Exploits sowie die Erstellung des Berichts wurden insgesamt 12 Personentage benötigt.

Der Zweck dieser Netzwerksicherheitsbewertung [redacted] war es, Sicherheitslücken zu identifizieren und die Wirksamkeit der auf die Anwendungen und Netzwerke angewandten Sicherheitskontrollen zu testen. Die Bewertung wurde mit teilweisem Wissen durchgeführt und unter der Annahme der Identität eines Angreifers, der in der Lage ist, die Anwendungen und Netzwerkgeräte effektiv zu kompromittieren.

Im Verlauf dieses Penetrationstests wurden **6 kritische, 3 hohe, 6 mittlere und 2 niedrige Schwachstellen** festgestellt

Dieses Dokument wird die Ergebnisse der Sicherheitsbewertung zusammenfassen, einschließlich der Sicherheitslücken und der Wirksamkeit der vorhandenen Sicherheitskontrollen. **Für detailliertere Informationen können die vollständigen Sicherheitsbewertungsberichte herangezogen werden.**

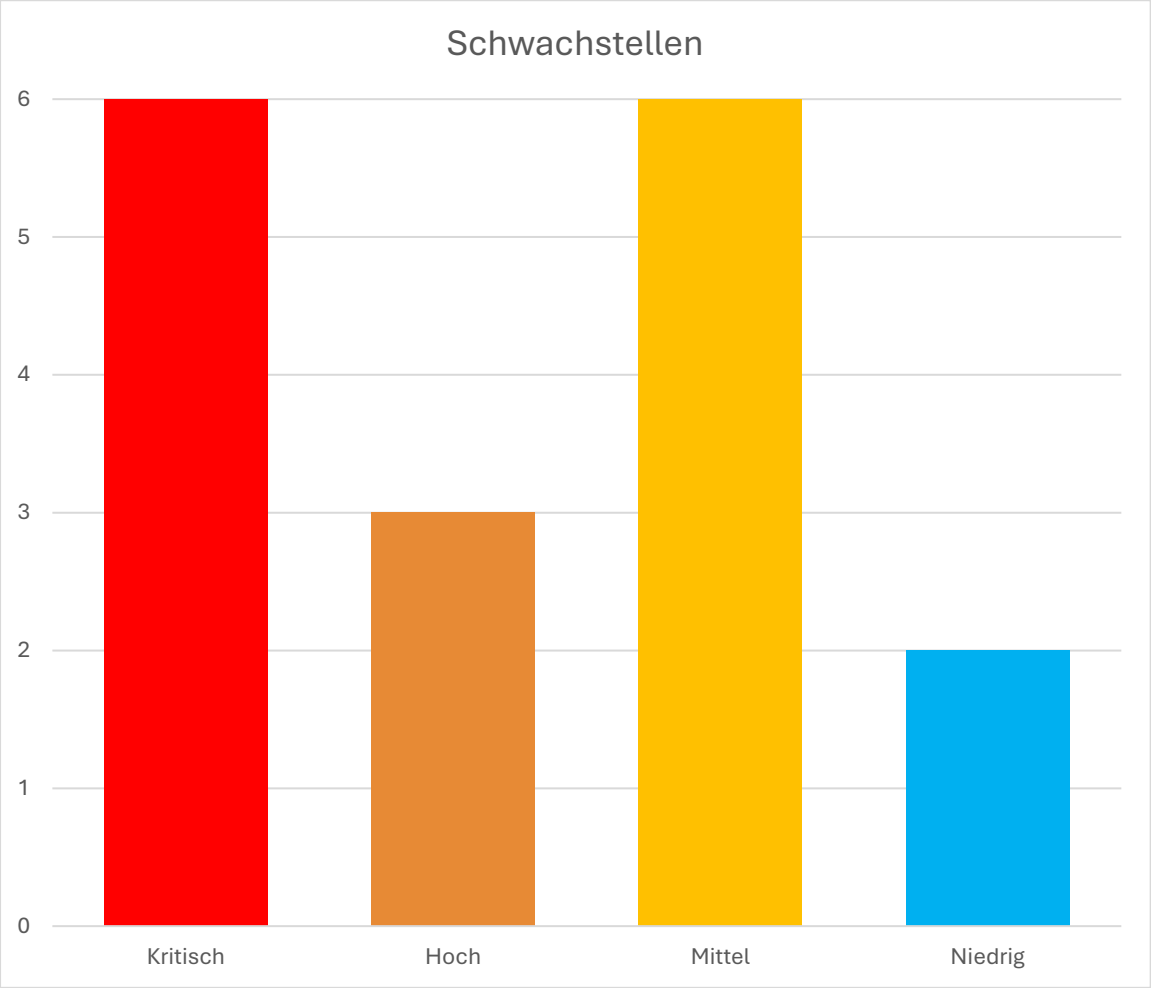

Abbildung 1 : Anzahl der Schwachstellen

Kritische Schwachstellen des Netzwerks

Während des Penetrationstests wurden insgesamt 6 kritische Schwachstellen entdeckt, [redacted] kompromittieren könnten. Diese Schwachstellen können die Integrität des Unternehmensnetzwerks ernsthaft gefährden.

C1, C2 Und C3: Standard-[redacted]Zugangsdaten

Netzwerkgeräte von [redacted], wie Switches, Router und andere Hardware, werden oft mit vorinstallierten Standard-Zugangsdaten (z. B. [redacted] ausgeliefert. Wenn diese nach der Installation nicht geändert werden, bieten sie einen einfachen Zugang für Angreifer. Ein Angreifer kann dann Netzwerkeinstellungen manipulieren, Hintertüren schaffen, Daten abfangen oder Netzdienste stören. Administratorzugriff wurde mit den oben genannten Standard-Kombinationen für die folgenden Systeme erlangt:

[redacted]

[redacted]

[redacted]

Weitere Einzelheiten zu dieser Schwachstelle finden Sie im Sicherheitsbewertungsbericht.

C4 und C5: Remotecodeausführung (Remote Code Execution)

Der [redacted] (HTML5) weist eine Remotecodeausführungs-Schwachstelle in einem [redacted]. Ein Angreifer mit Netzwerkzugriff auf Port 443 kann diese Schwachstelle ausnutzen, um Befehle mit uneingeschränkten Rechten auf dem Betriebssystem des vCenter Servers auszuführen. Betroffen sind [redacted]

Eine kritische Remotecodeausführungs-Schwachstelle im [redacted]

[redacted] entsteht durch fehlende Eingabevalidierung im Virtual SAN Health Check-Plugin. Angreifer mit Netzwerkzugriff auf Port [redacted] können Befehle mit vollen Rechten auf dem Betriebssystem ausführen. CVE-2021-21985 hat einen CVSSv3-Wert von 9.8.

Weitere Einzelheiten zu dieser Schwachstelle finden Sie im Sicherheitsbewertungsbericht.

C6: Microsoft Message Queuing RCE

Der Microsoft Message Queuing-Dienst auf dem entfernten Host ist von einer Remotecodeausführungs-Schwachstelle betroffen. Ein nicht authentifizierter Angreifer kann diese Schwachstelle ausnutzen, um über eine speziell gestaltete Nachricht beliebigen Code auf dem entfernten Host auszuführen.

Um diese Schwachstelle auszunutzen, müsste der Angreifer ein speziell gestaltetes bösartiges [redacted] was zur Ausführung von Code auf der Serverseite führen könnte.

Weitere Einzelheiten zu dieser Schwachstelle finden Sie im Sicherheitsbewertungsbericht.

Hochgradige Schwachstellen des Netzwerks

Im Zuge dieser Penetration wurden **3 Schwachstellen** entdeckt, die als hoch bewertet werden können.

H1 und H2: SMB Signing deaktiviert

SMB Signing deaktiviert bezieht sich auf eine Sicherheitslücke im Server Message Block (SMB)-Protokoll, das häufig für die Freigabe von Dateien und die Kommunikation zwischen Netzwerkgeräten verwendet wird.

Die Kernschwachstelle von SMB gegenüber Relay-Angriffen liegt im Authentifizierungsmechanismus, insbesondere bei der Nutzung von [redacted]. Angreifer können Authentifizierungsversuche abfangen und an einen anderen Server weiterleiten, um Benutzer zu imitieren. Dies ist möglich, wenn SMB Signing deaktiviert ist, da die Quelle oder das Ziel der Authentifizierungsanforderung nicht überprüft wird.

Anforderungen für einen Angriff:

[redacted]

Die folgenden IPs waren anfällig für SMB-Relay-Angriffe:

- [redacted]
- [redacted]

H3: SSH-Protokoll-Authentifizierungs-Bypass

Der entfernte ssh-Server ist anfällig für einen Authentifizierungs-Bypass. Ein Angreifer kann die Authentifizierung umgehen, indem er anstelle [redacted], die normalerweise die Authentifizierung einleitet, die [redacted] sendet.

Diese Schwachstelle wurde in einem Lorem ipsum bekannt gegeben, aber es wurde auch beobachtet, dass sie auf andere Anwendungen und Softwarepakete anwendbar ist.

Verwenden Sie [redacted] um den Exploit zu überprüfen.

Weitere Einzelheiten zu dieser Schwachstelle finden Sie im Sicherheitsbewertungsbericht.

Mittlere Schwachstellen des Netzwerks

Im Verlauf der internen Netzwerktests wurden **6 Schwachstellen** entdeckt, die als mittel klassifiziert werden können

M1, M2 und M3: Series Switches Software mehrfache Schwachstellen

Schwachstellen in der Weboberfläche der Series Switches-Software ermöglichen es einem entfernten, nicht authentifizierten Angreifer, Benutzer auf bösartige Websites umzuleiten. Dies geschieht aufgrund unzureichender Eingabevalidierung in HTTP-Anfragen. Angreifer können Anfragen abfangen und ändern, um den Benutzer auf eine schädliche URL weiterzuleiten. Diese Schwachstelle wird als Open-Redirect-Angriff bezeichnet und häufig in Phishing-Angriffen genutzt, um Benutzer unwissentlich auf schädliche Seiten zu locken.

Weitere Einzelheiten zu dieser Schwachstelle finden Sie im Sicherheitsbewertungsbericht.

M4, M5 und M6: Standard-FTP-Anmeldedaten

Die Verwendung von Standard- Zugangsdaten in FTP-Servern (File Transfer Protocol) stellt ein erhebliches Sicherheitsrisiko dar. Standard-Zugangsdaten [redacted], sind weithin bekannt und können von böswilligen Akteuren leicht ausgenutzt werden. Wenn diese Standard-Anmeldeinformationen nach der Ersteinrichtung nicht geändert werden, können unbefugte Benutzer vollen Zugriff auf den FTP-Server erhalten. Dieser Zugriff kann zu Datendiebstahl, unbefugten Datei-Uploads/Downloads und in einigen Fällen zur vollständigen Kontrolle über den Server führen.

Im Folgenden sind die angreifbaren Ziele und Standard-Zugangsdaten aufgelistet.

Username: [redacted] Password: [redacted]

[redacted]

[redacted]

Weitere Einzelheiten zu dieser Schwachstelle finden Sie im Sicherheitsbewertungsbericht.

Niedrige Schwachstellen des Netzwerks

Im Verlauf des Penetrationstests wurden 2 Schwachstellen gefunden, die als niedrig kategorisiert wurden.

L1 SSL Medium Strength Cipher Suites Unterstützt (SWEET32)

Der Remote-Host unterstützt die Verwendung von SSL- Verschlüsselungen, die eine mittlere Verschlüsselungsstärke bieten. Als mittelstark gilt jede Verschlüsselung, die Schlüssellängen von mindestens 64 Bit und weniger als 112 Bit verwendet oder die 3DES-Verschlüsselungssuite einsetzt.

Beachten Sie, dass es wesentlich einfacher ist, eine mittelstarke Verschlüsselung zu umgehen, wenn sich der Angreifer im selben physischen Netzwerk befindet.

L2 SSH-Server CBC-Modus- Verschlüsselungen aktiviert

Der SSH-Server ist so konfiguriert, dass er die Cipher Block Chaining (CBC)-Verschlüsselung unterstützt. Dies könnte es einem Angreifer ermöglichen, die Klartextnachricht aus dem Chiffretext wiederherzustellen. CBC-Modus-Cipher sind anfällig für kryptografische Angriffe wie [redacted] Daher gilt die Nutzung von CBC-Verschlüsselung als unsicher.

Die folgenden Hosts zeigen, dass die schwachen Verschlüsselungssuiten aktiviert wurden :

Weitere Einzelheiten zu dieser Schwachstelle finden Sie im Sicherheitsbewertungsbericht.

Haftungsausschluss

Die in diesem Bericht enthaltenen Informationen sind vertraulich und können rechtlich privilegiert sein. Sie sind ausschließlich für den Adressaten bestimmt, und der Zugriff auf diesen Bericht durch andere Personen ist nicht autorisiert. Wenn Sie nicht der beabsichtigte Empfänger sind, ist jede Offenlegung, Vervielfältigung, Verbreitung oder Handlung, die auf dieser Information basiert, untersagt und kann rechtswidrig sein.

NetzExperten Unternehmensberatung GmbH & Co. KG haftet nicht für Verluste, die aus Ereignissen entstehen, die außerhalb unserer angemessenen Kontrolle liegen. Wir übernehmen keine Haftung für Geschäftsverluste, einschließlich, aber nicht beschränkt auf Verlust oder Beschädigung von Gewinnen, Einkommen, Einnahmen, Nutzung, Produktion, erwarteten Einsparungen, Geschäft, Verträgen, kommerziellen Möglichkeiten oder Firmenwert, oder sonstige Verluste, die durch die Nutzung oder den Missbrauch dieses Berichts entstehen.