CloudCommand

Cyber Security

CloudCommand GmbH chr.schumacher@gmx.tm

Cyber Security im Unternehmens-umfeld

CloudCommand GmbH chr.schumacher@gmx.tm

Übersicht Netzwerk-sicherheit

Übersicht über Netzwerksicherheit

- Stabile Sicherheitsvorkehrungen sind erforderlich, um verdächtige Ereignisse, Angriffe und Schwächen in Ihrem Netzwerk erkennen und verhindern zu können. Sicherheitsrelevante Probleme können aus den verschiedensten Gründen entstehen und es gibt auch verschiedene Möglichkeiten, mit ihnen umzugehen. Im Folgenden werden die verschiedenen Arten von Netzwerksicherheitsstrategien untersucht, die Sie zur Bewältigung dieser Probleme einsetzen können.

Zugriffssteuerung

- Im Rahmen der Zugriffssteuerung können Sie alle Benutzer*innen und Clients überprüfen, um zu beurteilen, ob sie berechtigt sind, auf Ihr Netzwerk oder die darin enthaltenen Ressourcen zuzugreifen. Sie implementieren die Zugriffssteuerung durch das Konfigurieren von Sicherheitsrichtlinien, die dafür sorgen, dass Benutzer*innen genau die Berechtigungen zugewiesen werden, die erforderlich sind, um bestimmte Aktionen in Ihrem Netzwerk auszuführen. Ein Beispiel wäre, dass Sie den Lesezugriff auf bestimmte Ressourcen verweigern möchten, wenn ein Benutzer außerhalb des lokalen Standorts eine Verbindung herstellen möchte.

Anti-Schadsoftware-Tools

- Anti-Schadsoftware-Tools schützen Ihr Netzwerk vor Schadsoftware (Malware). Schadsoftware kann verschiedene Formen annehmen, z. B.:
  - Ransomware
  - Viren
  - Spyware
  - Trojaner
- Sie können Anti-Schad- und Anti-Virussoftware verwenden, um Schadsoftware zu überwachen und zu entfernen. Diese Tools können Anomalien in Ihren Dateien feststellen, Aktionen ausführen, um schädliche Codebestandteile zu entfernen, und betroffene Ressourcen und Geräte in Ihrem Netzwerk reparieren.

Anwendungssicherheit

- Angreifer können Anwendungen kompromittieren, unabhängig davon, ob es sich dabei um Ihre eigenen Anwendungen oder um Anwendungen von Drittanbietern handelt. Möglicherweise enthält eine Software versehentlich Sicherheitslücken, über die ein Angreifer auf Geräte und Netzwerkressourcen zugreifen kann.
- Wenn eine Anwendung direkt in Ihrem Unternehmen entwickelt wird, sollten Sie selbst aktiv dafür sorgen, Sicherheitslücken zu identifizieren und zu schließen, die Angreifer ausnutzen könnten.

Anwendungssicherheit

- Eine mögliche Lösung ist das Testen Ihrer Anwendung während des Entwicklungslebenszyklus und das Implementieren aller Änderungen, die erforderlich sind, um mögliche Sicherheitsrisiken zu beseitigen.
- Wenn es sich um eine Anwendung handelt, die von einem Drittanbieter entwickelt wurde, sollten Sie Updates immer sofort installieren, sobald diese verfügbar sind.

Verhaltensanalysen

- Sie können Tools für Verhaltensanalysen verwenden, um regelmäßige Nutzungs- und Verhaltensmuster in Ihrem Netzwerk zu bestimmen und verdächtige Änderungen zu erkennen.
- Beispielsweise könnten Sie feststellen, dass ein Benutzer plötzlich damit beginnt, von seinen gewöhnlichen Nutzungsmustern abweichend auf Ihr Netzwerk zuzugreifen. Normalerweise greift der Benutzer von einem Standort in den Vereinigten Staaten und während seiner regulären Arbeitszeit auf das Netzwerk zu. Wenn seine Anmeldeinformationen plötzlich um Mitternacht für Anmeldeversuche aus Australien verwendet werden, wird dieser Versuch als verdächtig gekennzeichnet.

Verhaltensanalysen

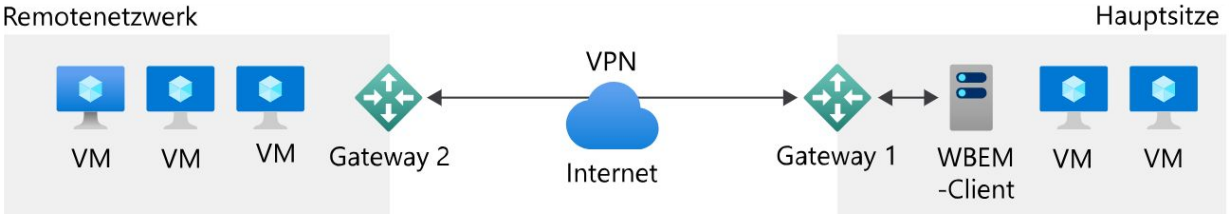
- Basierend auf diesen Analysen können Sie Sicherheitsrichtlinien erstellen, um dieses Problem anzugehen. Sie könnten beispielsweise festlegen, dass der Zugriff so lange verweigert wird, bis eine zusätzliche Überprüfung durchgeführt wurde, z. B. in Form eines geheimen Codes, der an das geschäftliche Mobilgerät des Nutzers gesendet wird.

Erkennen und Verhindern von Eindring-Versuchen

- Für Ihr Netzwerk empfiehlt sich eine proaktive und präventive Sicherheitsstrategie. Je früher Sie einen Eindringversuch erkennen, desto besser kann damit umgegangen werden. Sie können Tools für das Erkennen und die Verhinderung von Eindringversuchen in Kombination verwenden, um den gesamten Datenverkehr in Ihrem Netzwerk zu überwachen.

VPN

- Ein virtuelles privates Netzwerk (VPN) kann eine verschlüsselte Verbindung zwischen Netzwerken über das Internet herstellen. Das VPN konfiguriert einen verschlüsselten Tunnel, über den sichere Kommunikation über TLS oder IPSec hergestellt wird und in dem Ihnen Funktionen für Remotezugriff in Ihren Netzwerken zur Verfügung stehen.



Websicherheit

- Es können Tools bereitgestellt werden, die für eine sichere Verwendung des Internets durch Ihre Benutzer sorgen. So können Sie beispielsweise ein Webfilter verwenden, damit Benutzer bestimmte Arten von Websites nicht aufrufen können, die ein Sicherheitsrisiko darstellen.
- Über diese Websicherheitstools können Sie außerdem Richtlinien einrichten, die Ihnen bei der Entscheidung helfen, wie verschiedene Arten von Webanforderungen in Ihrem Netzwerk verarbeitet werden sollen.

WLAN

- Drahtlos betriebene Bestandteile Ihres Netzwerks sind nicht so sicher wie über Kabelverbindungen betriebene Bestandteile. Auf ein Drahtlosnetzwerk kann je nach Stärke des Funksignals auch von außerhalb Ihrer Organisation zugegriffen werden.
- Ihnen stehen verschiedene Tools zur Verfügung, mit denen Sie Aktivitäten in den drahtlos betriebenen Teilen Ihres Netzwerks überprüfen und überwachen können.

WLAN

- Der erste Schritt bei der Sicherung eines Drahtlosnetzwerks ist die Verwendung des stärksten Verschlüsselungstyps, der auf Drahtlosgeräten verfügbar ist.
- Konfigurieren Sie dann ein eigenständiges Drahtlosnetzwerk für Gäste, damit Besucher nicht das Drahtlosnetzwerk verwenden können, das für interne Benutzer vorgesehen ist.

CloudCommand

CloudCommand GmbH chr.schumacher@gmx.tm