CloudCommand

Cyber Security

CloudCommand GmbH chr.schumacher@gmx.tm

Cyber Security im Unternehmens-umfeld

CloudCommand GmbH chr.schumacher@gmx.tm

Netzwerk-sicherheit Authentifi-zierung

Netzwerkauthentifizierung

- Nur authentifizierte und autorisierte Benutzer oder Dienste sollten auf Netzwerkressourcen zugreifen. Der Zugriff muss auf der Authentifizierung und Autorisierung basieren.
- Die Netzwerkauthentifizierung ist so zu konfigurieren, dass überprüft wird, ob es sich tatsächlich um den angemeldeten Benutzer handelt. Die Authentifizierung führt zur Unterscheidung zwischen legitimen und verdächtigem Zugriffen innerhalb ihres Netzwerkes. Es gibt unterschiedliche Methoden die Authentifizierung zu implementieren.

Netzwerkauthentifizierung

Kennwortauthentifizierung

- Der Benutzer vergibt eine Zeichenfolge, welche nur ihm bekannt ist, um auf das Netzwerk zuzugreifen.
- Sichere Kennwörter müssen bestimmte Kriterien erfüllen, z. B.
  - Klein- und Großbuchstaben
  - Zahlen
  - Zeichen (wie ?, % oder $)

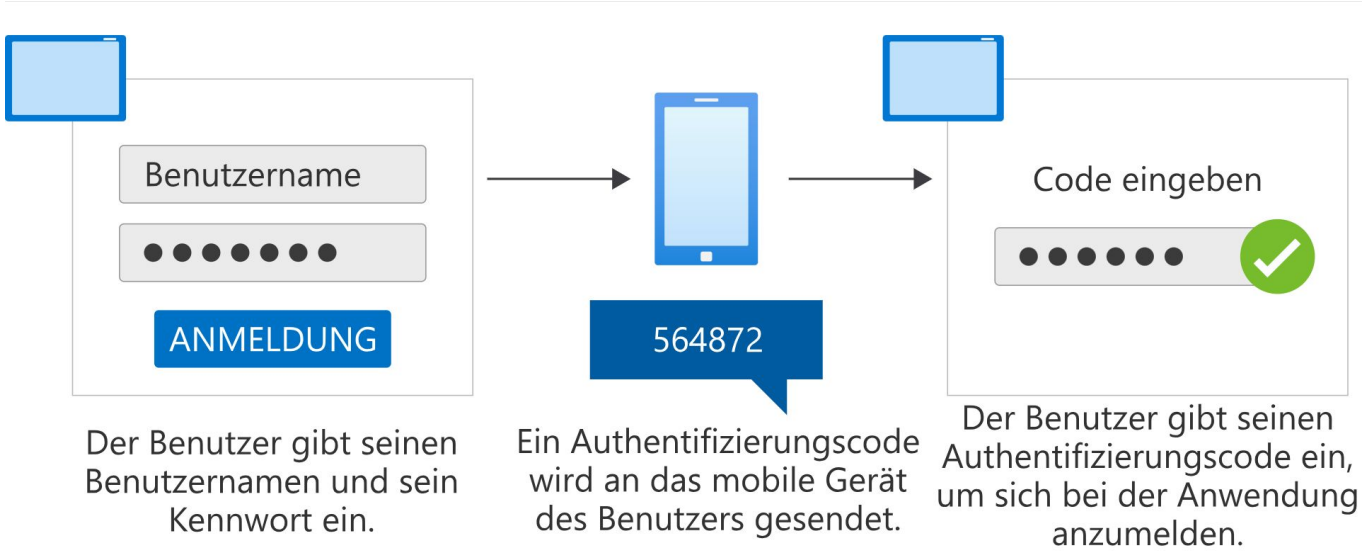
Es wird außerdem empfohlen, möglichst lange Kennwörter zu verwenden.

Netzwerkauthentifizierung

Zweistufige Authentifizierung

- Die zweistufige Authentifizierung ist ein Mechanismus, mit dem Benutzer einen Authentifizierungsversuch verifizieren können. Der Benutzer muss einen Einmalcode zur Bestätigung der Authentifizierung angeben, der an sein Gerät gesendet wird. Dieser Code wird beispielsweise per Textnachricht gesendet oder durch einen Code über eine App wie Microsoft Authenticator auf einem Smartphone generiert.

Netzwerkauthentifizierung



Netzwerkauthentifizierung

Tokenauthentifizierung

- Die tokenbasierte Authentifizierung ähnelt der zweistufigen Authentifizierung. Anstelle eines Smartphones, das kompromittiert werden könnte, kann ein Unternehmen ein Gerät verwenden, das ausschließlich für die Authentifizierung gedacht ist. Bei diesem Token kann es sich um ein USB-fähiges Gerät oder eine Smartcard handeln, die Benutzer für die Authentifizierung verwenden. Unternehmen, die eine tokenbasierte Authentifizierung verwenden, sollten sicherstellen, dass der Benutzer das Gerät zurückgibt, wenn er den Zugriff nicht länger benötigt.

Netzwerkauthentifizierung

Biometrische Authentifizierung

- Bei der biometrischen Authentifizierung werden die physischen Attribute des Benutzers für die Authentifizierung verwendet. Dabei handelt es sich um eindeutige menschliche Merkmale wie Fingerabdrücke, Gesichtszüge oder die Stimme. Wegen der spezifischen Art von Scanner, der für die Bearbeitung dieser Art von Informationen erforderlich ist, kann die Implementierung der biometrischen Authentifizierung jedoch teuer sein. Bedenken zum Datenschutz der Benutzer können ebenfalls Probleme darstellen.

Netzwerkauthentifizierung

Transaktionale Authentifizierung

- Vielleicht möchten Sie sich nicht immer nur auf Informationen verlassen, die von Benutzern angegeben werden. Stattdessen werden bei der transaktionalen Authentifizierung die Merkmale von Benutzern überprüft. Sie könnten beispielsweise davon ausgehen, dass Benutzer immer während ihrer Arbeitszeit aus den USA auf das Netzwerk zugreifen. Wenn jedoch um Mitternacht eine Anmeldung von der anderen Seite der Welt erfolgt, wird das Konto des Benutzers markiert, und das System fordert den Benutzer dazu auf, zusätzliche Schritte für die Authentifizierung durchzuführen.
- Die transaktionale Authentifizierung bietet somit eine zusätzliche Schutzschicht für Ihr Netzwerk.

Netzwerkauthentifizierung

Netzwerkauthentifizierung

CAPTCHA

- Mit einem CAPTCHA (Completely Automated Public Turing test /to tell Computers and Humans Apart, vollautomatischer öffentlicher Turing-Test zur Unterscheidung von Computern und Menschen) wird überprüft, ob die Entität, die versucht auf ein System zuzugreifen, ein Mensch ist.

Netzwerkauthentifizierung

- Angreifer können Anwendungen erstellen, die in der Lage sind, die Anmeldung Schritte bei Konten zu automatisieren. Ein CAPTCHA stellt ein verzerrtes Bild von Szenarien, Buchstaben oder Zahlen dar, und Benutzer müssen angeben, was im Bild gezeigt wird. Anders als Menschen haben Anwendungen Schwierigkeiten mit der Identifikation von verzerrten Fotos, Buchstaben und Zahlen. Menschen können in der Regel erkennen, worum es sich bei einem verzerrten Bild handelt.
- Denken Sie jedoch daran, dass diese Methode Benutzern mit Sehschwäche Probleme bereiten kann.

Netzwerkauthentifizierung

Einmaliges Anmelden (Single-Sign-On)

- Bei der einmaligen Anmeldung geben Benutzer Ihre Anmeldeinformationen einmal an, um sich für mehrere Anwendungen und Tools zu authentifizieren.
- Benutzer können sich beispielsweise bei ihrer E-Mail-Anwendung anmelden und automatisch für die Tools authentifiziert werden, die sie zum Verwalten der Netzwerksicherheit und des -speichers nutzen. Mit dem einmaligen Anmelden sparen Ihre Benutzer Zeit.
- Bei dieser Methode besteht jedoch die Gefahr, dass das einmalige Anmelden einem Angreifer dabei helfen kann, sich Zugriff auf mehrere Plattformen, Tools und Anwendungen zu verschaffen, wenn er sich erfolgreich Zugriff auf nur eine dieser Anwendungen verschafft.

Netzwerkauthentifizierung

Authentifizierungsprotokolle

- Ein Authentifizierungsprotokoll beschreibt ein gemeinsames Regelwerk für den Austausch von Informationen zwischen elektronischen Geräten. Zwei der am häufigsten verwendeten Authentifizierungsprotokolle sind Kerberos und Transport Layer Security/Secure Sockets Layer (TLS/SSL).

Netzwerkauthentifizierung

Kerberos

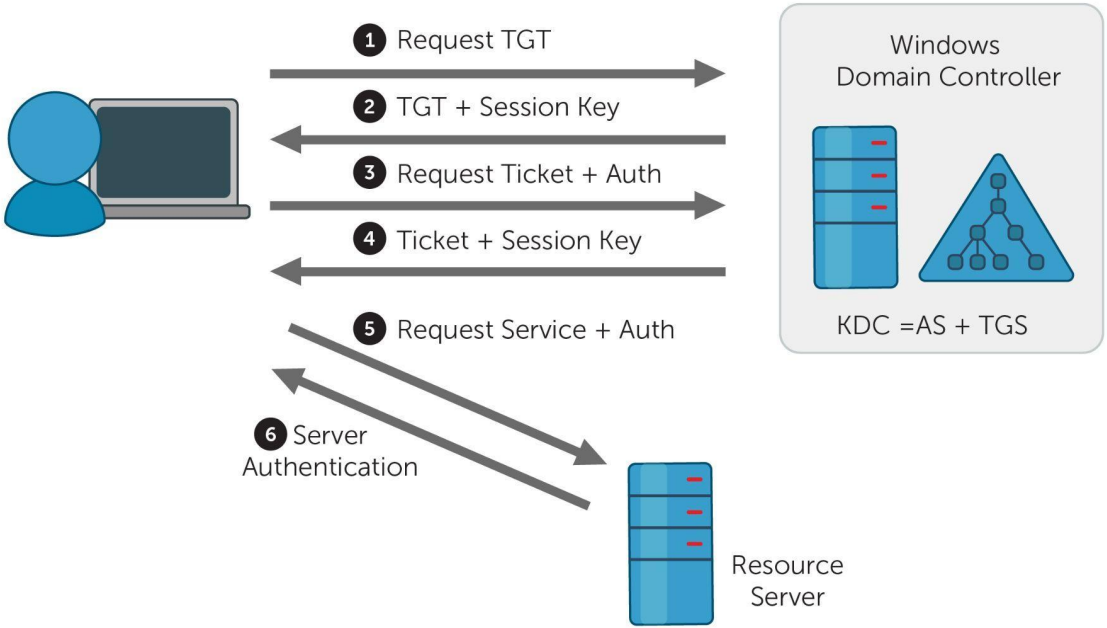
- Kerberos ist ein Authentifizierungsprotokoll, das auf verschiedenen Betriebssystemen verwendet wird. Kerberos ist unter Windows das Standard Authentifizierungsprotokoll. Linux und Mac OS können Kerberos ebenfalls verwenden.
- Das Kerberos-Authentifizierungsprotokoll basiert auf einem vertrauenswürdigen Server, der als Schlüsselverteilungscenter (Key Distribution Center – KDC) bezeichnet wird. Ein KDC besteht aus mehreren Komponenten:

Netzwerkauthentifizierung

- in Authentifizierungsserver, der die Authentifizierung durchführt und wie ein Benutzer oder Dienst Tickets an Prinzipale übergibt
- eine Datenbank, die Informationen über die Prinzipale und deren geheime Schlüssel enthält
- ein weiterer Server, der Dienst-Tickets basierend auf den ursprünglichen Tickets erteilt, die von den Prinzipalen übermittelt werden

- In Kerberos rufen Prinzipale Tickets ab, die ihnen die Dienst-Tickets vom KDC übergeben. Diese Dienst-Tickets werden für den Zugriff auf Ressourcen, Dienste oder Anwendungen verwendet. Dieser Prozess ist für Benutzer nicht sichtbar.

Netzwerkauthentifizierung



Netzwerkauthentifizierung

TLS/SSL (Transport Layer Security/Secure Sockets Layer)

- Das TLS- und das ältere SSL-Protokoll sind beide für die Verschlüsselung von Informationen vorgesehen, die über das Internet gesendet werden. Da diese Daten verschlüsselt sind, können Angreifer nicht sehen, was über TLS/SSL übermittelt wird.
- Im Browser wird oft ein Vorhängeschloss Symbol angezeigt, wenn eine Website eine sichere Verbindung nutzt. Dieses Symbol gibt an, dass die Website eine sichere TLS/SSL-Sitzung mit dem Browser verwendet. TLS/SSL wird außerdem für Datenübertragungen, Voice-over-IP und E-Mails verwendet.
- SSL ist der veraltete Vorgänger von TLS. Beide Begriffe werden jedoch meist austauschbar verwendet. Die Protokolle funktionieren wie folgt:

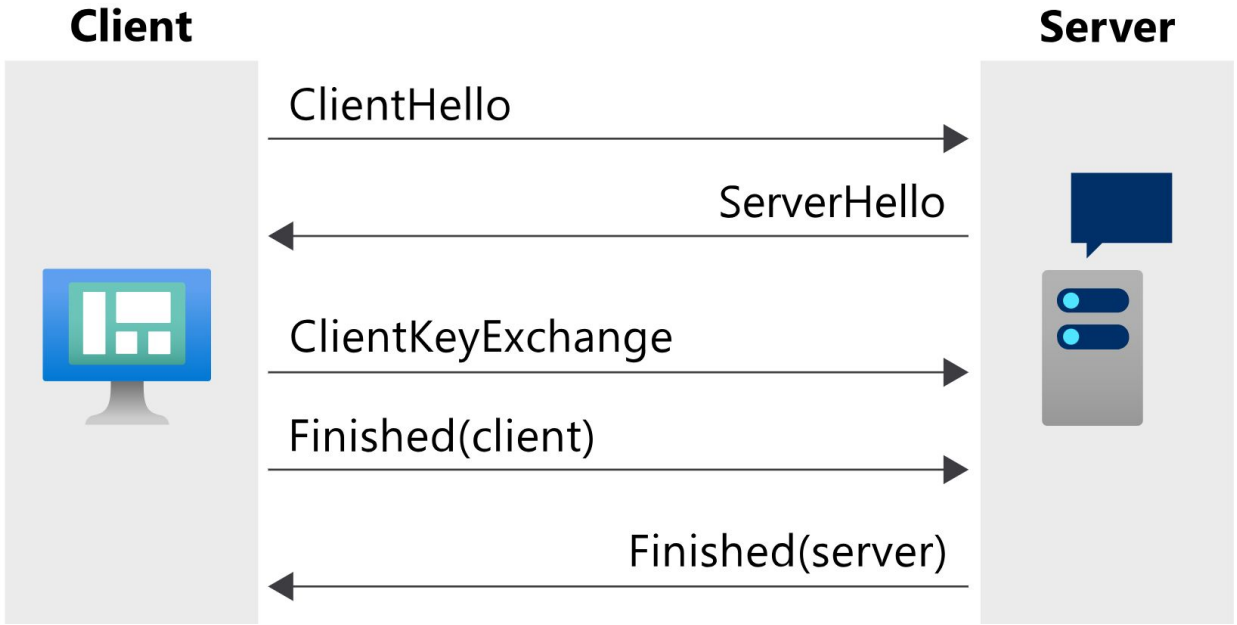
Netzwerkauthentifizierung

1. Der Client sendet die Nachricht „ClientHello“ an den Server. Diese Nachricht enthält Informationen wie die SSL/TLS-Version und die vom Client unterstützten Kryptografiealgorithmen.
2. Der Server sendet die Nachricht „ServerHello“ zurück, die den Algorithmus enthält, der aus der Liste der vom Client unterstützten Algorithmen ausgewählt wurde. Die Nachricht enthält außerdem eine Sitzungs-ID, das digitale Zertifikat des Servers und den öffentlichen Schlüssel.
3. Der Client verwendet das digitale Zertifikat, um die Identität des Servers anhand einer Zertifizierungsstelle zu verifizieren, damit der Client sich sicher sein kann, dass er mit einem vertrauenswürdigen Server interagiert.

Netzwerkauthentifizierung

4. Ein Client Schlüsselaustausch findet statt, bei dem der Client einen gemeinsam verwendeten Schlüssel an den Server sendet, der mit dem öffentlichen Schlüssel des Servers verschlüsselt wurde.
5. Der Client sendet eine „Abgeschlossen“-Nachricht, die mit dem gemeinsam verwendeten Schlüssel verschlüsselt wurde.
6. Der Server sendet eine eigene „Abgeschlossen“-Nachricht, die ebenfalls mit dem gemeinsam verwendeten Schlüssel verschlüsselt wurde. Ab diesem Punkt können der Client und der Server weiterhin Nachrichten austauschen, die mit dem gemeinsam verwendeten Schlüssel verschlüsselt sind.

Netzwerkauthentifizierung



Netzwerkautorisierung

- Nachdem die Authentifizierung erfolgreich abgeschlossen wurde, müssen Sie sicherstellen, dass die authentifizierten Benutzer*innen oder der authentifizierte Client für den Zugriff auf die angeforderten Ressourcen oder Dienste autorisiert ist. Diese Autorisierung kann genau abgestimmt werden.
- Ein bestimmter Datenbankbenutzer kann beispielsweise über die Berechtigungen verfügen, um auf eine einzelne Datenbank zuzugreifen und Änderungen an dieser vorzunehmen. Der Benutzer wäre jedoch nicht in der Lage, auf andere Datenbanken zuzugreifen, da er nicht über die Berechtigungen verfügt.

Netzwerkautorisierung

- Die Berechtigungen können Lese-, Schreib-, Lösch Berechtigungen und mehr umfassen. Verwenden Sie die richtigen Berechtigungen für den entsprechenden Benutzer oder Client. Wenn einem Benutzer oder Client eine neue Rolle zugewiesen wird, können Sie seine Berechtigungen an die neue Zugriffsebene anpassen.
- Sie sollten jedem Benutzer oder Client nur die für das Ausführen seiner Aufgaben mindestens erforderlichen Berechtigungen zuweisen. Vermeiden Sie es unbedingt, einem Benutzer oder Client Berechtigungen zuzuweisen, die er nicht benötigt.

Authentifizierung vs. Autorisierung

Authentifiszierung

- Überprüft, ob der Benutzer oder Client derjenige ist, für den er sich ausgibt
- Fordert Anmeldeinformationen wie Benutzername oder Kennwort an
- Muss vor der Autorisierung durchgeführt werden
- Angenommen, ein Mitarbeiter der Personalabteilung meldet sich bei der Personal-App an

Authentifizierung vs. Autorisierung

Autorisierung

- Überprüft, ob der Benutzer oder Client Aktionen in Bezug zu einer Ressource oder einem Dienst durchführen kann
- Überprüft die Berechtigungen, die dem Konto im Hintergrund zugeordnet sind, und gibt manchmal an, welche Berechtigungen man benötigt
- Erfolgt nach erfolgreicher Authentifizierung
- Er versucht versehentlich, einen Benutzer aus der falschen Abteilung zu löschen. Diese Aktion wird verweigert, da er nicht über die entsprechenden Berechtigungen für die betreffende Abteilung verfügt

CloudCommand

CloudCommand GmbH chr.schumacher@gmx.tm