CloudCommand

Cyber Security

CloudCommand GmbH chr.schumacher@gmx.tm

Cyber Security im Unternehmens-umfeld

CloudCommand GmbH chr.schumacher@gmx.tm

Grundlagen Physischer Sicherheit

Grundlagen Physischer Sicherheit

- Zugangsbeschränkungen
  - Kontrolle
- Überwachungssysteme
  - Überwachung
- Sicherheitsrichtlinien
  - Testen

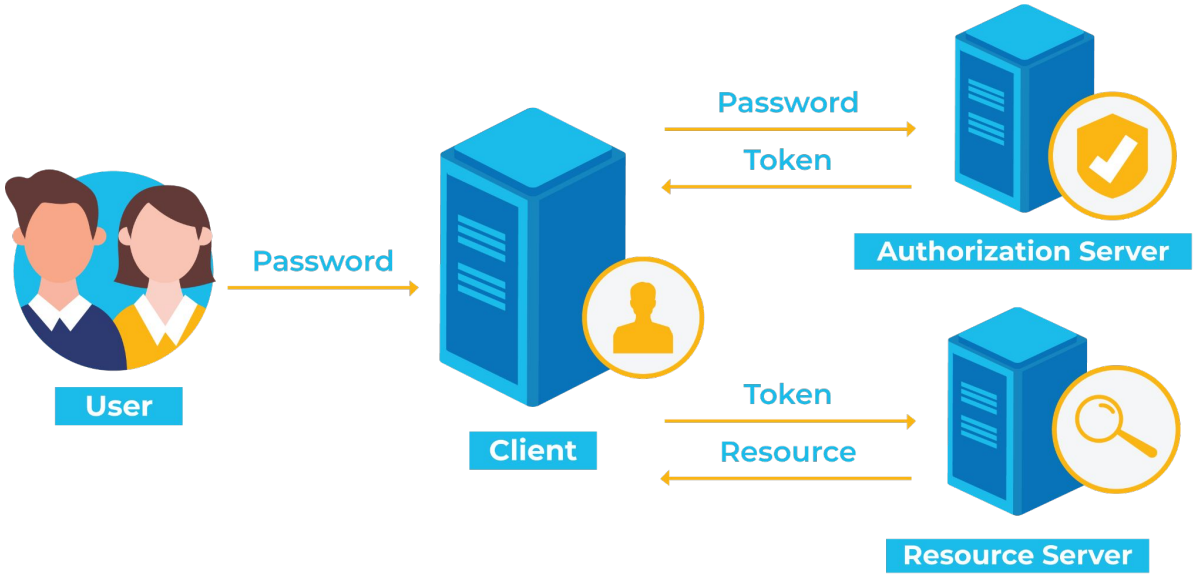
Zugangsbeschränkungen: Technologische Zugangskontrolle

- Wiegand Zugangskarten
- Barcode/QR Code
- Magnetstreifenkarten
- RFID Zugangskarten
- Smartcard

Zugangsbeschränkungen: Tokenbasierte Authentifizierung

- Der Benutzer erhält ein Token, das den Zugriff für einen bestimmten Zeitraum gewährt.
- Das Token kann verschiedene Formen haben: verbunden (z.B. USB, NFC, Smartphones)
- Vorteil:
  - Geringerer Speicherbedarf auf dem Server
  - Diebstahl des Tokens ist schwieriger

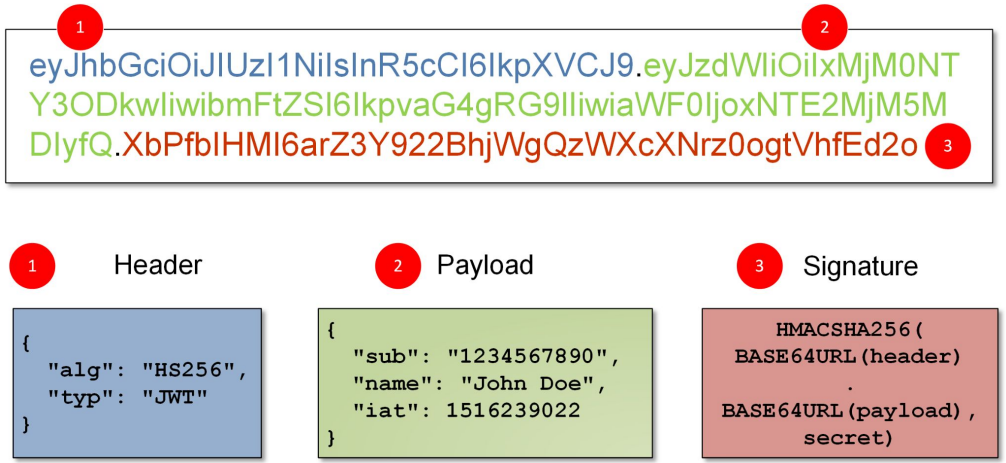
Zugangsbeschränkungen: Tokenbasierte Authentifizierung



Zugangsbeschränkungen: JSON Web Token (JWT)

- JWTs sind ein offener Standard (RFC 7519) für sichere Datenübertragung zwischen Parteien.
- **Header:** Enthält den Typ des Tokens und Signaturalgorithmus
- **Payload:** Trägt Claims/Behauptungen (z.B. Benutzeridentität)
- **Signatur:** Digitale Signatur, die die Integrität des Tokens sicherstellt.

Zugangsbeschränkungen: JSON Web Token (JWT)



Zugangsbeschränkungen: Technologische Zugangskontrolle

Gesichtserkennung vs. Fingerabdruck-Scanning

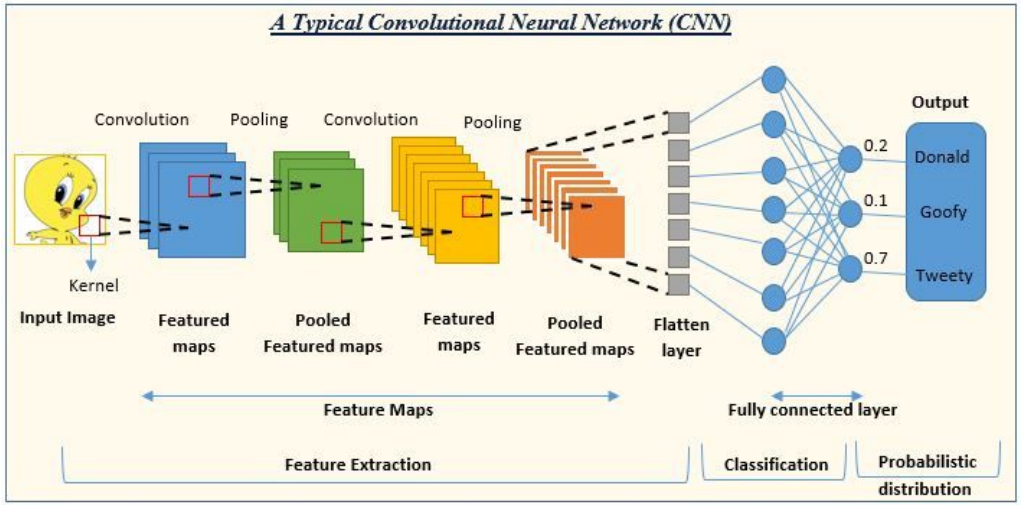
Zugangsbeschränkungen: Gesichtserkennung

- Nutzung von Gesichstmkermale wie Augenabstände, Nasenform und Wangenknochenstruktur.
- Verwendung von 2D bzw. 3D Modellierung
- Algorithmen
    - Convolutional Neural Networks (CNNs)

Zugangsbeschränkungen: Convolutional Neural Networks (CNNs)

- Convolutional Layer:
  - Reihe von Filtern
  - Filter erfassen merkmale wie Ecken und Kanten
- Faltung (Convolution):
  - Elementenweise Multiplikationen
  - hervorgehobene Merkmale
- Pooling Layer:
  - Reduktion der Dimensionalität
- Fully Connected Layer:
  - Aggregieren und Verarbeiten von Merkmale (Klassifizierung)

Zugangsbeschränkungen: Convolutional Neural Networks (CNNs)



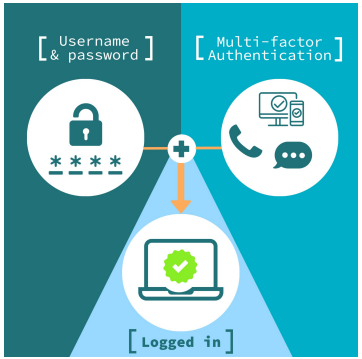
Zugangsbeschränkungen: Fingerabdruck-Scanning

- Fingerabdruck wird durch Rillen, Wirbel und andere Fingerkuppen-Merkmale erfasst
  - Optische Sensoren nutzen Licht für Aufnahme
  - Kapazitive Sensoren messen elektrische Signale
  - Ultraschallbasierte Sensoren erfassen 3D Bilder
- Der Abdruck wird digitales Format umgewandelt
  - Darstellung aus Minutienpunkten
- Überprüfung
  - Minutienpunktevergleich
- Herausforderungen
  - Schlechte Qualität durch Fingerfeuchtigkeit, Alter, Beschädigungen
  - Sicherheitsrisiken und Datenschutz

Zugangsbeschränkungen: Multifaktor-Authentifizierung

Multi-Faktor-Authentifizierung (MFA) ist eine Authentifizierungsmethode, bei der der Benutzer zwei oder mehr Verifizierungsfaktoren angeben muss, um Zugang zu einer Ressource wie einer Anwendung, einem Online-Konto oder einem VPN zu erhalten.

- Erhöhte Sicherheit
- Schutz vor Phishing und Brute-Force-Angriffen
- Reduzierung von Identitätsdiebstahl
- Verbesserung der Compliance
- Flexibilität und Anpassungsfähigkeit
- Steigerung des Vertrauens
- Schutz vor Remote-Zugriff



Zugangsbeschränkungen: Für Mitarbeiter und Besucher

Mitarbeiter:

- interne WLAN-Netzwerk
- Unternehmens Anmeldeinformationen
- Kundeninformationen
- Datenbanken
- spezielle geschützte Netzwerke

Zugangsbeschränkungen: Für Mitarbeiter und Besucher

Externe Anbieter/Dienstleister:

- externes Anbieter-WLAN
- Authentifizierung über temporäre Zugangscodes
- Überwachung und Protokollierung von Aktivitäten

Besucher/Gäste

- separates Gast-WLAN
- temporärer Zugang
- keine internen Ressourcen erreichbar

Zugangsbeschränkungen: Zugriffskontrollmodelle

Role-Based Access Control (RBAC):

- Rollen definieren
- Rollen erhalten spezifische Berechtigungen für Ressourcen
- Zugriff basiert auf Benutzerrollen und zugehörigen Berechtigungen.
- Effiziente Verwaltung durch Rollenzuweisungen.

Zugangsbeschränkungen: Zugriffskontrollmodelle

Attribute-Based Access Control (ABAC):

- Entscheidungen basieren auf Benutzerattributen und Kontext.
- Nutzt Attribute wie Rollen, Standort, Zeit, Sensitivität der Daten.
- Erlaubt feingranulare Kontrolle über Ressourcenzugriffe.
- Berücksichtigt diverse Attribute für Zugriffsentscheidungen.

Zugangsbeschränkungen: Protokollierung von Zugriffen

Eine systematische Erfassung und Speicherung von Zugriffsdaten auf Ressourcen, Systeme und physische Bereiche

Identifizierung von Zugriffen

- Dokumentierung von Zugriffsversuchen

Protokollierung

- Aktivitätsaufnahme Operationen wie Read, Write, Delete

Zeitstempel

- Erfassung des Zeitpunkts eines Ressourcenzugriffs

Authentifizierungsstatus

- Zugriffserfolg bzw. -fehlschlag

Überwachungssysteme

Verschiedene Sensoren, Instrumente und Technologien bilden ein System zur Überwachung von Aktivitäten, Systemen und Ereignissen. Die Daten werden gesammelt, analysiert und für wichtige Sicherheitszwecke aufgezeichnet.
Zwecke der Überwachung:

- Sicherheit: Schutz kritischer Ressourcen, Verhinderung von Vandalismus, Diebstahl usw.
- Schadenprävention: Erkennung potenzieller Gefahren
- Kontrolle von Arbeitsabläufen, Arbeitsleistung und Einhaltung von Richtlinien
- Dokumentation für rechtliche Zwecke
- Haftungsschutz

Arten von Überwachungskameras

Analoge Kameras:

- Übertragen Videosignale über Koaxialkabel oder Twisted-Pair-Kabel.
- Auflösung: 480 oder 720p.
- Die Signale werden auf einem DVR (Digital Video Recorder) übertragen
- Geringere Anfälligkeit für Cyberangriffe durch fehlende IP-Adressen und Software
    - Keine Internetverbindung

Arten von Überwachungskameras

Digitale Kameras:

- übertragen Videosignale über Netzwerkkabel (Ethernet oder drahtlos über Wi-Fi / Bluetooth) an Netzwerk-Videorekorder (NVR) oder an einen Server.
- Möglichkeit für Aufnahme Speicherung auf SD-karte
- CCD (Charge-Coupled Device) oder CMOS (Complementary Metal-Oxide Semiconductor) erfassen Licht und wandeln es in elektronische Signale um.
- bieten sofortige Anzeige und höhere Bildqualität
- IP- Kameras (Internet Protocol-Kamera)

Vorteile von Überwachungssystemen

Evidenz
- Beweismaterial bei Vorfälle

Kontrolle
- Arbeitsprozesse kontrollieren

Überblick
- parallele Beobachtung

Arbeitssicherheit
- Gefahrenerkennung und prevention

Prävention von Straftaten

Nachteile von Überwachungssystemen

Privatsphäre

- Unbewilligten Zugriff auf die Privatsphäre

Missbrauch

- Verkauf sensibler Daten oder unbefugte nutzung der Daten

Kosten:

- Installation, Wartung, Schutz

Technische Probleme

Trends und Zukunftsaussichten Künstlicher Intelligenz

Höhere Auflösung

- Upscaling-Technologien:
  - Mit Machine Learning werden Muster erkannt und zusätzliche Details/Pixeln hinzugefügt
- Bildverbesserungsalgorithmen:
  - Rauschen reduzieren
  - Kontrast, Helligkeit, Farben anpassen

Personalisierte Erfahrungen

- Priorisieren von Objekte, Personen, Ereignisse
- adaptive Benachrichtigungen etc.

Erstellung von Sicherheitsrichtlinien

Eine Sicherheitsrichtlinie oder Security-Richtlinie ist ein Dokument, in dem schriftlich festgehalten wird, wie ein Unternehmen seine physischen und informationstechnischen (IT) Vermögenswerte schützen will.

Sicherheitsrichtlinien sollen dynamisch sein und mit der Zeit aktualisiert werden!

Inhalt von Sicherheitsrichtlinien

Acceptable Use Policy (AUP):

- Regeln für die Nutzung von Ressourcen
- Beispiele:
  - Verbot der Installation nicht autorisierter Software
- Instrument zur Durchsetzung von Sicherheitsmaßnahmen
  - Sanktionen

Inhalt von Sicherheitsrichtlinien

- Zugangsregelungen:
  - Passwortrichtlinien,
  - mehrstufige Authentifizierung
  - Berechtigungsstufen
- Beispiel:
  - Zugriffsrechte für neu eingestellte Mitarbeiter

Inhalt von Sicherheitsrichtlinien

- Effektivitätsbewertung
  - Festlegung der Bewertungsmethoden
  - Frequenz der Bewertung
  - Verantwortlichkeiten
  - Dokumentation der Ergebnisse
  - Maßnahmen zur Verbesserung
  - Aktualisierung

Inhalt von Sicherheitsrichtlinien

- Schulungen und Sensibilisierungsmaßnahmen
  - Arten von Sensibilisierungs-
  - maßnahmen beschreiben
  - Zielgruppen und
  - Häufigkeit
  - Inhalte der Schulungen
  - Verantwortlichkeiten:
  - Evaluierung
  - Konsequenzen

Inhalt von Sicherheitsrichtlinien

- Incident Response Plan (Reaktionsplan bei Vorfällen)
  - Ziel und Umfang
  - Verantwortlichkeiten und Zuständigkeiten
  - Schritte und Verfahren
  - Kommunikation
  - Testen und Aktualisieren
  - Compliance und Berichterstattung

CloudCommand

CloudCommand GmbH chr.schumacher@gmx.tm