Zero Trust

Ein Überblick über das IT-Sicherheitskonzept

Linux-Café

01. Juni 2022

Inhalt

- IT-Sicherheitskonzepte
- Wo ist das Problem?
- Wer hat's erfunden?
- Was kann es?
- Wie ist es aufgebaut?
- Einführung von Zero Trust
- Zusammenfassung/Ausblick

IT-Sicherheitskonzepte

Einige Begriffe

- Informationssicherheit
  - Maßnahmen zur Sicherstellung von
    - Vertraulichkeit
    - Verfügbarkeit
    - Integrität
    - (Authentizität)
    - (Verbindlichkeit)

    } Schutzziele

    in technischen und nichttechnischen Systemen
  - IT-Grundschutz (Bundesamt für Sicherheit in der Informationstechnik (BSI))
- Sicherheitskonzept
  - Aufeinaner abgestimmte Maßnahmen, die in ihrer Kombination die gewünschte Schutzwirkung erzielen
  - Maßnahmen können technisch, organisatorisch, baulich oder auch versicherungstechnischer Natur sein
- Gesetzliche Anforderungen
  - IT-Sicherheitskonzepte sind für bertreiber kritischer Infrastrukturen vorgeschrieben
- Informationssicherheits-Managementsystem (IMSI)
  - Erfordert zwingend u. a. ein IT-Sicherheitskonzept

Wo ist das Problem?

Klassischer Ansatz zur Sicherheit in vernetzten Systemen (1)

- Unterscheidung internes (gutes) Netz / externes (böses) Netz
  - Interne Clients werden anders behandelt als externe
  - Viele Dienste sind nur im internen Netz zu erreichen
  - Voraussetzung für den Zugriff von außen ist ein VPN ins interne Netz
- Implizite Annahmen
  - Das Nutzerverhalten ist dem Standort (intern/extern) zuzuordnen
    - eigene Mitarbeiter sind gut, andere böse
  - Anhand des Standorts (intern/extern) lassen sich Annahmen über die Berechtigungen eines Clients treffen
    - intern gut → Zugriff auch auf Infrastrukturkomponente
    - extern böse

Wo ist das Problem?

Klassischer Ansatz zur Sicherheit in vernetzten Systemen (2)

- Realität
  - Auch interne Clients oder Nutzer sind potentiell eine Gefahr für die IT-Sicherheit
    - Schädlingsbefall
    - Böswilligkeit
    - Technische Fehler (Exploits)
  - Angreifer, die in das interne Netz eingedrungen sind, haben umfassende Möglichkeiten, Schaden zu verursachen
- Schlussfolgerung
  - Unterteilung internes / externes Netz ist nicht ausreichend für die gewünschte Qualität der IT-Sicherheit
- Alternativer Ansatz: Zero Trust
  - Prämisse: Die Clients dürfen aufgrund ihrer Position im Netz keine besonderen Rechte genießen

Wer hat's erfunden?

Was gibt es / Wie wird es benannt?

- Zero Trust Security Model
- Zero Trust Architecture (ZTA)
- Zero Trust Networt Architecture (ZTNA)
- (auch Perimeterless Security)

Historie

- Erstmals 1994 in der Doktorarbeit von Stephen Paul Marsh an der University of Stirling benutzt.
- 2003 vom Jericho Forum wieder aufgegriffen bei der Arbeit an „de-perimiterisation“.
- 2009 von Google in der „BeyondCorp“ implementiert.
- Seit 2010 vermehrt in der Diskussion zur Stärkung der „Cyber-Security“.
- Seit 2020 verstärktes Interesse aufgrund der Pandemie-bedingten Öffnung von Firmen-Netzen

Zero Trust: Definition

- National Institute of Standards and Technology (NIST)
  - NIST Special Publication 800-207: Zero Trust Architecture (https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-207.pdf)
  - National Cybersecurity Center of Excellence (NCCoE): Projekt: Implementing a Zero Trust Architecture (https://www.nccoe.nist.gov/projects/implementing-zero-trust-architecture)
  - National Cyber Security Center (NCSC): Alternativer Ansatz für Zero Trust auf Basis von
    - Eine einzige verlässliche Quelle zur Sicherstellung der Benutzer-Identität
    - Benutzer-Authentifizierung
    - Geräte-Authentifizierung
    - Zusätzlicher Kontext, wie z. B. Einhaltung von Richtlinien und Gerätezustand
    - Autorisierungsrichtlinien für den Zugriff auf eine Anwendung
    - Zugriffsrichtlinien innerhalb einer Anwendung

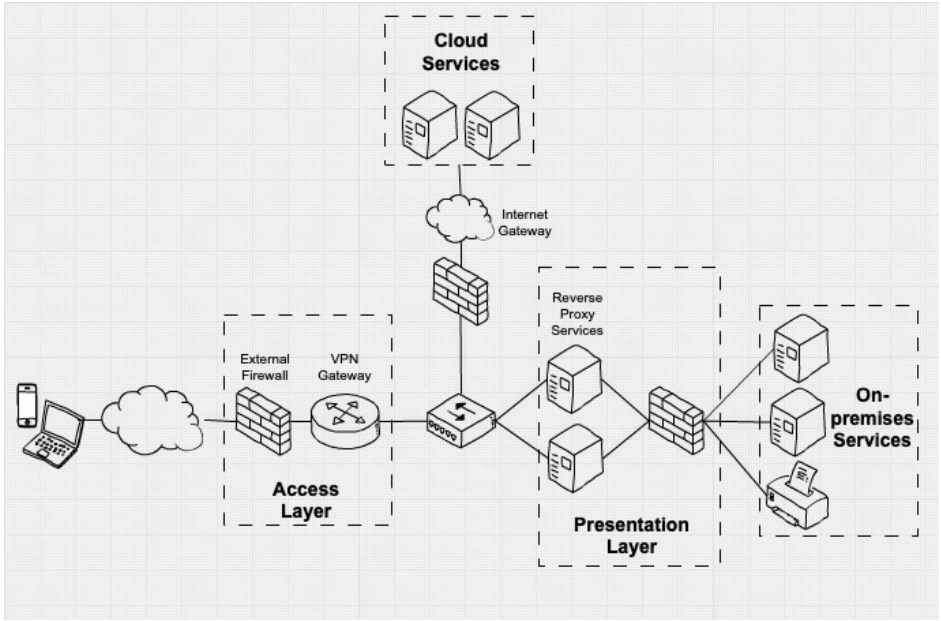
    (https://www.ncsc.gov.uk/collection/device-security-guidance/infrastructure/network-architectures)

Was kann es?

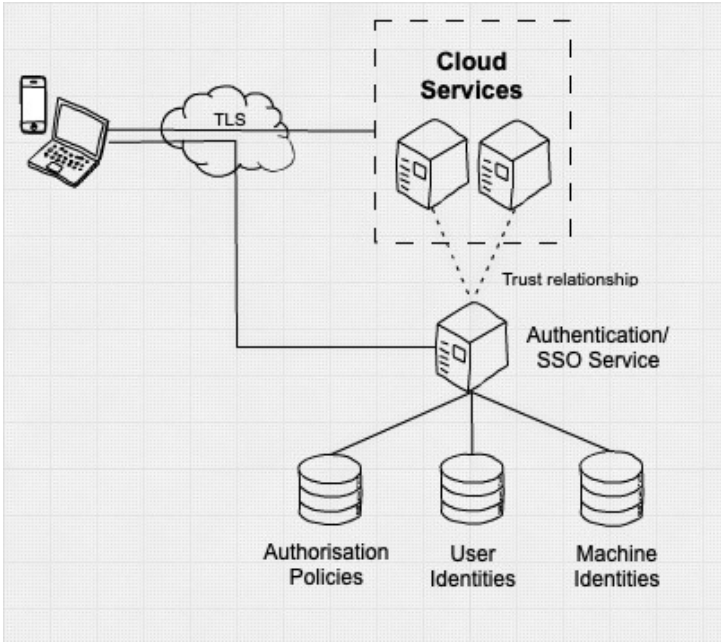
- Zero Trust Grundsatz:
  - Vertraue nie
  - Überprüfe immer
- Keine Aufteilung in
  - Sicheres internes Netz
  - Unsicheres externes Netz
- Mutual Authentication / Gegenseitige Authentifizierung
  - Überprüfung der Identität und Integrität
  - ohne Rücksicht auf die Netzwerk-Lokation
- Zugriff auf Dienste auf Basis von Vertrauen in die
  - Identität und Integrität in Verbindung mit
  - Benutzer-Verifikation

National Cyber Security Center (NCSC): Alternativer Ansatz für Zero Trust

Konventioneller VPN-basierter Fernzugriff



Zero-Trust-Architektur



Wie ist es aufgebaut?

Bausteine eines Zero Trust Konzepts

- Clients müssen stets angemeldet / authentifiziert sein
- ausgefeiltes Rechtekonzept mit zentraler Verwaltung
  - Zentrale Benutzerverwaltung: LDAP oder Active Directory
  - Rollen- und Rechtekonzept
    - Herausforderung: Grenzen durch Beschränkung auf Gruppen-basierte Regelwerke
    - Vorausschauende Planung unter Einbeziehung der für die Anwender geforderten notwendigen Dienste
- sämtliche Netzwerkverbindungen müssen verschlüsselt sein

- ggf. kann zusätzlich auch eine VPN genutzt werden, um spezielle Dienste weiter abzuschotten

NIST SP800-207: 7 Grundsätze (1)

1. Ressourcen-Vielfalt
   - nicht nur Endpunkte / Server sind Ressourcen
   - auch (Cloud-)Dienste sind relevant
   - für alle sind grundlegende/erweiterte Authentifizierungs- und Zugriffskontrollen notwendig
2. Kommunikationsabsicherung
   - Zero Trust Network Access: alle Zugriffe sind gesperrt, außer bei expliziter Freigabe
   - Alle anderen Ressourcen sind „unsichtbar“
3. Einmalzugriff
   - Zugriffe werden nicht dauerhaft gewährt, sondern sind (z. B. für jede Session) neu zu verifizieren
4. Dynamische Policies
   - Statische Regelwerke sind nicht geeignet, Zugriffe hinreichend zu beschränken
   - Auswertung dynmischer Informationen („Signale“), wie z. B. Standort, Benutzer, Gerät, Anwendungskontext

NIST SP800-207: 7 Grundsätze (2)

5 Security Monitoring

- Laufende Überwachung der Sicherheitslage und ggf. (dynamische) Anpassung der Zugriffsegeln

6 Strikte Einhaltung

- Laufende Neubewertung des Vertrauens zur Durchsetzung der Richtlinien

7 Soviel Daten wie möglich

- Laufende Überwachungsfunktion um Informationen über Assets, Netzwerkinfrastruktur und Kommunikation zur dynamischen Verarbeitung in
  - Policy Engine
  - Policy Administration
  - Policy Enforcement Point

  zu generieren.

  (Siehe auch Blog des Software Engineering Institute der Carnegie Mellon University)

Einführung von Zero Trust

Schrittweises Herangehen

1. Definition der zu schützenden Objekte
   - Sensible Objekte identifizieren: Daten, Anwendungen, Assets, Dienste
   - Weitere Angriffsflächen müssen nicht unbedingt mit Zero Trust gesichert werden
2. Abbildung der Datenflüsse
   - Notwendig, um zu bestimmen, wie die Zugriffe geschützt werden müssen
3. Aufbau einer Zero Trust Architektur
   - Individuelle Architektur definiert sich über die Schutzfläche und die Datenflüsse
   - Möglicher erster Ansatz: Next Generation Firewall (Layer 7)
4. Festlegung des Regelwerks
   - Wer, Was, Wann, Wo, Warum und Wie
5. Überwachung und Wartung
   - Kontinuierliche Überwachung der Betriebsparameter und Anpassung des Systems

Wo klemmt es?

Herausforderungen bei der Einführung von Zero Trust Konzepten

- Schwammige Definition des einzigen verfügbaren Standards SP800-207 (NIST)
- Nicht jeder Dienst kann fein genug an die notwendige Rechteverwaltung angepasst werden
  - fehlende LDAP-Unterstützung
  - proprietäre/legacy Anwendungen
  - Mögliche Lösung: Proxys (z. B. Teleport) zur Anbindung älterer Lösungen
- Handhabung von „Mobile Devices“
  - Gerade Smartphones würden davon provitieren, kein VPN nutzen zu müssen
  - Sicherheit der Geräte muss dabei gewährleistet sein (Diebstahl, ...)
  - Zentrale Administration der Smartphones aktuell aber nur über die proprietären Lösungen von Google und Apple sinnvoll möglich

Zusammenfassung

Was macht ein Zero Trust Sicherheitskonzept aus?

- Umstellung von netzwerk- zu endpunktbasiertem Zugangsmodell
  - Endpunkte können Geräte, Dienste oder Anwendungen sein
- Es gibt kein Vertrauen
  - Jeder Zugriffsversuch wird anhand von Richtlinien auf die Zulässigkeit geprüft und nur mit den minimal notwendigen Rechten erlaubt.

Ausblick

Beyond Zero Trust

- Zero Trust eXtended (ZTX) (2018, Forrester Research): Weiterentwickeltes Framework
  - sensible Daten identifizieren und ihren Fluss darstellen
  - klären, wer, wann, wo, warum und wie auf Daten zugreift und was mit ihnen gemacht wird
  - konsequent datenzentrischer Ansatz mit konstantem Monitoring
- BeyondCord (Google)
  - 2009 innerhalb von Google entwickelt und intern verwendet
  - seit 2019 wird es auch Kunden angeboten
- CARTA (Continuous Adaptive Risk and Trust Assessment) (2017, Gartner)
  - Nutzer, Geräte und Anwendungen werden nicht nur bei der Anmeldung, sonder laufend überwacht und ggf. eingegriffen
- Software Defined Parameter (SDP)
  - Aufbau der Netzwerkverbindungen nach dem „Need-to-Know-Prinzip“
  - Kombination aus Geräte-Authentifizierung, identitätsbasiertem Zugang und dynamischer Konnektivität
  - Nutzung bekannter Ansätze wie Next Generation Firewall, Network Access Control, 802.1x-Standard