

9 Attack and Defence Scenarios

Defence-in-depth:

- Koordinierter Einsatz mehrerer Sicherheitsmaßnahmen um Unternehmen zu schützen
- komplexes und Vielschichtiges System
- Kompensiert potentielle menschliche Fehler




minimiert Wahrscheinlichkeit, dass Hacker mit Angriff erfolgreich sind. Bei erfolgreichem Angriff

Zero Trust Kernprinzipien

1. Modern Work Enablement
2. Goal Alignment
3. Risk Alignment
4. People Guidance and Inspiration
5. Risk and Complexity Reduction
6. Alignment & Automation
7. Security for the Full Lifecycle
8. Asset-Centric Security
9. Least privilege
10. Simple and Pervasive
11. Explicit trust Validation

Zero Trust

- Sicherheitskonzept mit Grundsatz, dass keinem Gerät, Nutzer, Dienst intern als auch extern vertraut wird
- Vergabe von so wenig Rechten wie nötig
- Grundsätzlich Verschlüsselung
- Analyse von Netzwerkverkehr
- Assume Breach
- Sämtliche Aktionen loggen
- Grundsätzliches Misstrauen

Unterschied herkömmlicher Konzepte  Dienste, Nutzer, Anwendungen werden im eigenen Netzwerk als vertrauenswürdig eingestuft

Zero Trust gebote

- Vertrauen ausdrücklich bestätigen (mittels Informationen und Telemetrie)
- Moderne Arbeit ermöglichen (Enable, nicht blockieren)
- Durchgängige Sicherheit ermöglichen (Sicherheit in Unternehmenskultur, Normen und Prozesse integrieren)
- Assets nach Wert absichern (Angemessener Schutz von Business Assets in Bezug auf ihren Business Wert und das erwartete Risiko)

- Einführung von Asset-bezogenen Kontrollen (Präzise Kontrollen auf Assets abgestimmte und nicht nur Infrastrukturweite standard Kontrollen)
- Einfache und Nachhaltige Sicherheit (Maßnahmen sollten so einfach wie möglich gehalten werden und dabei gleichzeitig paraktisch, skalierbar und nachhaltig sein)
- Möglichst niedrige Rechte verwenden (Zugriff nur wenn wirklich benötigt vergeben, wenn nicht mehr benötigt wieder entziehen)
- Dauerhaft verbessern (permanent weiterentwicklen und verbessern da sich IT permanent verändert)
- Fundierte Entscheidungen treffen (Entscheidung auf Grundlage der bestmöglichen Informationen treffen)

Microsoft Zero Trust Prinzipien

- **Explizit verifizieren**
 - Benutzer Identität und Location
 - Geräte Zustand (Compliance)
 - Kontext, in dem Informationen abgerufen werden
 - Daten Klassifikationen
 - Jegliche Anomalien
- **Zugriff mit geringsten Rechten verwenden**
 - Just in Time (JIT)
 - Just enough Access (JEA)
 - Risikobasierte adaptive Policy
- **Schwachstellen annehmen**
 - Segmentierung von Netzwerken, Benutzern, Geräten, Services, ... vornehmen
 - Sitzungen Ende-zu-Ende verschlüsseln
 - Analysen zu Gefahrenerkennung verwenden und Verteidigung verbessern zu können

[Gute Quelle](#)

"Das Sichere Unternehmensnetzwerk" gibt es nicht mehr.