CloudCommand

Cyber Security

CloudCommand GmbH chr.schumacher@gmx.tm

Motivation Cyber Security

CloudCommand GmbH chr.schumacher@gmx.tm

Defense-in-Depth

Was ist Defense-in-Depth (DiD)?

Defense-in-Depth ist ein Sicherheitskonzept, das darauf abzielt, ein System oder Netzwerk durch mehrere Schutzebenen zu sichern. Anstatt sich ausschließlich auf eine einzelne Sicherheitsmaßnahme zu verlassen, werden mehrere Schichten von Verteidigungsmechanismen implementiert, um potenzielle Angriffe abzuwehren.

Worauf basiert das Konzept?

Das Konzept basiert auf der Idee, dass selbst wenn eine Schutzmaßnahme umgangen wird, andere Sicherheitsvorkehrungen immer noch greifen können, um den Angriff zu stoppen oder abzuschwächen.

Diese Schutzebenen können physische Sicherheitsmaßnahmen, Firewalls, Intrusion Detection Systems, Verschlüsselung, Zugriffskontrollen und andere Technologien umfassen.

Was bietet Defense-in-Depth?

Defense-in-Depth bietet eine umfassende Sicherheitsstrategie, die es Angreifern erschwert, in ein System einzudringen und Schaden anzurichten. Durch die Kombination verschiedener Sicherheitsmaßnahmen auf verschiedenen Ebenen wird die Sicherheit insgesamt gestärkt und das Risiko von erfolgreichen Angriffen reduziert.

Architektur von Defense-in-Depth?

Die Defense-in-Depth-Sicherheitsarchitektur basiert auf Kontrollen, die die physischen, technischen und administrativen Aspekte Ihres Netzwerks schützen sollen.

Architektur von Defense-in-Depth?

Physische Kontrollen: Diese Kontrollen umfassen Sicherheitsmaßnahmen, die den physischen Zugang zu IT-Systemen verhindern, wie z. B. Sicherheitspersonal oder verschlossene Türen.

Technische Kontrollen: Zu den technischen Kontrollen gehören Sicherheitsmaßnahmen, die Netzwerksysteme oder -ressourcen mit spezieller Hardware oder Software schützen, z. B. eine Firewall oder ein Antivirenprogramm.

Administrative Kontrollen: Administrative Kontrollen sind Sicherheitsmaßnahmen, die aus Richtlinien oder Verfahren bestehen, die sich an die Mitarbeiter einer Organisation richten, z. B. die Anweisung an die Benutzer, sensible Informationen als "vertraulich" zu kennzeichnen.

Architektur von Defense-in-Depth?

Darüber hinaus tragen die folgenden Sicherheitsebenen zum Schutz einzelner Aspekte Ihres Netzes bei:

- **Zugriffsmaßnahmen:** Zu den Zugriffsmaßnahmen gehören Authentifizierungskontrollen, Biometrie, zeitlich begrenzter Zugriff und VPN.
- **Arbeitsplatzschutz:** Zu den Arbeitsplatzschutzmaßnahmen gehören Antiviren- und Antispam-Software.
- **Datenschutz:** Zu den Methoden des Datenschutzes gehören Data-at-Rest-Verschlüsselung, Hashing, sichere Datenübertragung und verschlüsselte Backups.

Architektur von Defense-in-Depth?

- **Perimeter Schutz:** Zu den Perimeter Schutzmaßnahmen gehören Firewalls, Intrusion Detection Systems und Intrusion Prevention Systems.
- **Überwachung und Vorbeugung:** Die Überwachung und Vorbeugung von Netzwerkangriffen umfasst die Protokollierung und Prüfung von Netzwerkaktivitäten, Schwachstellen-Scanner, Sandboxing und Schulungen zum Sicherheitsbewusstsein.

Anwendungsfälle

Im Großen und Ganzen lassen sich die Anwendungsfälle von Defense-in-Depth in Szenarien für den Benutzerschutz und Szenarien für die Netzsicherheit unterteilen.

Defense-in-Depth Benutzerschutz umfasst eine Kombination aus Sicherheitsangeboten (z. B. WAF, Antivirus- und Antispam-Software) und Schulungen, um Bedrohungen zu blockieren und wichtige Daten zu schützen.

Ein Anbieter von Software zum Schutz von Endbenutzern vor Cyberangriffen kann mehrere Sicherheitsangebote in einem Produkt bündeln. So kann er beispielsweise Virenschutz, Firewall, Spamschutz und Datenschutzkontrollen in einem Produkt vereinen.

Dadurch ist das Netzwerk des Benutzers gegen Malware und Angriffe aus Webanwendungen (z. B. XSS, CSRF) geschützt.

Anwendungsfälle

Sicherheit im Netzwerk

- Ein Unternehmen richtet eine Firewall ein und verschlüsselt zusätzlich die Daten, die durch das Netzwerk fließen, sowie die Daten im Ruhezustand. Selbst wenn Angreifer die Firewall überwinden und Daten stehlen, sind die Daten verschlüsselt.
- Ein Unternehmen richtet eine Firewall ein, betreibt ein Intrusion Protection System mit geschultem Sicherheitspersonal und setzt ein Antivirenprogramm ein. Dies bietet drei Sicherheitsebenen - selbst wenn Angreifer die Firewall überwinden, können sie vom IPS erkannt und gestoppt werden. Und wenn sie einen Endbenutzer-Computer erreichen und versuchen, Malware zu installieren, kann diese vom Antivirenprogramm erkannt und entfernt werden.

CloudCommand

CloudCommand GmbH chr.schumacher@gmx.tm