iTentity erklärt:

Zero Trust Security

Cyber Security Awareness Month

iTentity erklärt:

Was ist Zero Trust Security?

Zero Trust Security ist ein revolutionärer Ansatz zur IT-Sicherheit, der besagt: „Vertraue niemandem, überprüfe alles“.

Im Gegensatz zu traditionellen Sicherheitsmodellen, die internen Benutzern automatisch vertrauen, behandelt Zero Trust alle Zugriffe als potenziell unsicher, unabhängig davon, ob sie von innerhalb oder außerhalb des Netzwerks kommen.

iTentity erklärt:

Warum ist Zero Trust Security wichtig?

Verbesserte Sicherheit:
Minimiert das Risiko von Sicherheitsverletzungen durch kontinuierliche Überprüfung aller Zugriffe.

Schutz vor Insider-Bedrohungen:
Erlaubt keinen blinden Vertrauensvorschuss, selbst für interne Benutzer.

iTentity erklärt:

Warum ist Zero Trust Security wichtig?

Anpassung an moderne Arbeitsweisen:
Ideal für Remote-Arbeit und Cloud-Nutzung, wo traditionelle Perimeter-Sicherheit versagt.

Kleinere Angriffsfläche:
Reduziert potenzielle Angriffspunkte durch segmentierte Netzwerkzugriffe.

iTentity erklärt:

Wie lässt sich Zero Trust Security umsetzen?

Mikrosegmentierung:
Aufteilung des Netzwerks in kleinere, isolierte Segmente, um den Zugriff streng zu kontrollieren.

Strikte Zugangskontrollen:
Implementierung von Least Privilege Access – jeder Benutzer und jedes Gerät hat nur Zugriff auf das, was unbedingt erforderlich ist.

Kontinuierliche Überprüfung und Authentifizierung:
Jeder Zugriff wird ständig überprüft, egal ob es sich um einen internen oder externen Benutzer handelt.

iTentity erklärt:

Wie lässt sich Zero Trust Security umsetzen?

Mehrstufige Authentifizierung (MFA):
Nutzung von mehreren Faktoren zur Authentifizierung, wie z.B. Passwort und biometrische Daten.

Geräteüberprüfung und -überwachung:
Ständige Überwachung und Überprüfung von Geräten, die auf das Netzwerk zugreifen.

Datenschutz durch Verschlüsselung:
Verschlüsselung von Daten sowohl im Ruhezustand als auch während der Übertragung.

iTentity erklärt:

Wie lässt sich Zero Trust Security umsetzen?

Konsistente Überwachung und Logging:
Fortlaufende Überwachung von Netzwerkaktivitäten und Protokollierung aller Zugriffe.

Risikobasierte Zugriffsentscheidungen:
Bewertung des Zugriffs basierend auf dem aktuellen Risikolevel, z.B. anhand des Verhaltens des Benutzers oder der Anomalien.