ZERO TRUST

Es wird grundsätzlich keinem Nutzer oder Device vertraut – egal, ob intern oder extern. Der Zugriff wird nur nach strenger Authentifizierungs- und Zugriffskontrolle gestattet. Kommunikation mit anderen Netzwerkteilnehmern (menschliche oder technische) kommt nur bei entsprechender Berechtigung zustande.

PUBLIC TRUST

Öffentlich zugängliche Dienste wie Webseiten oder Social-Media-Plattformen, die für eine breite Öffentlichkeit erreichbar sind. Die meisten Nutzer und Geräte dürfen ohne strenge Zugriffskontrolle oder Authentifizierung zugreifen.

PRIVATE TRUST

Vertrauen wird nur bestimmten, internen Netzwerken oder Benutzergruppen gewährt. Der Zugriff wird durch Sicherheitsmaßnahmen wie Firewalls auf authentifizierte Quellen beschränkt. Unbekannte und externe Nutzer oder Geräte werden blockiert.

6.400

Google-Anfragen innerhalb eines Monats gibt es rund um das Thema Zero Trust.

15 MRD.

IoT-Devices weltweit sind 2023 schätzungsweise im Einsatz. Welchem davon kann man trauen?

It's time for Zero Trust.

Move forward with essendi xc.

Wie viele Identitäten haben Sie eigentlich in Ihrem Netzwerk?

XC UND ZERO TRUST

In einer Zero-Trust-Umgebung ist ein verlässliches Tool zur Authentifizierung notwendig. Um sich einem Zero-Trust-System gegenüber auszuweisen, benötigt man einen „Ausweis": ein digitales Zertifikat. Als vollumfängliches Zertifikatsmanagement-Tool stellt essendi xc digitale Zertifikate automatisiert nach festgelegten Compliance-Vorgaben aus und verteilt sie bis in die Zielsysteme (inkl. IoT/OT Devices). Er ist somit ein wesentlicher Grundpfeiler für eine sichere und reibungslose Kommunikation in Zero-Trust-Umfeldern.

XC