IT-TIPP

essendi it
IT-Beratung und -Entwicklung

# Nur keine Identitätskrise

## Digitale Identitäten als zentraler Bestandteil der IT-Sicherheit

**Um sich im Internet auszuweisen, benötigt man eine digitale Identität. Egal ob man Mensch, Maschine, Organisation oder Diensteanbieter ist. Was gilt es zu beachten, um in Zeiten steigender Digitalisierung kein Risiko einzugehen?**

Jeder Mensch ist ein unverwechselbares Individuum und eindeutig identifizierbar durch Wesensmerkmale wie Name, Aussehen, Größe oder Stimme. Eine Identität ist also die Summe aller Merkmale, anhand derer man Menschen eindeutig voneinander unterscheiden kann.

Auch eine digitale Identität (eID von electronic identity) kann als Summe an Informationen definiert werden, die benötigt werden, um den Menschen, das Gerät oder die Organisation zu identifizieren, der in der realen Welt hinter einer eID steht. Sie ist daher die Grundlage für die Wiedererkennung von Nutzern und für den Aufbau von Vertrauen in elektronischen Geschäfts- und Verwaltungsprozessen.

Da eIDs sich intern in Netzwerken oder extern im Internet bewegen, müssen die Informationen zur Identifikation von Computern verarbeitet und gespeichert werden können. Sie müssen also in digitaler Form vorliegen, wie Namen oder Gerätebezeichnungen, E-Mail- oder IP-Adressen und Passwörter.

### Digitale Identitäten schützen

Durch die zunehmende Digitalisierung ist der Umgang mit eIDs zu etwas ganz Alltäglichem geworden. Und obwohl sie tagtäglich sowohl privat als auch geschäftlich

Elektronische Identitäten sind ein schützenswertes Gut.

genutzt werden, wird ihr Schutz zumeist vernachlässigt. Hacker nutzen gestohlene eIDs privater User, um sich zu bereichern. Im Darknet floriert der Handel mit gestohlenen Maschinenidentitäten.

Gerade jetzt, wo durch Corona immer mehr Abläufe ins Netz verlagert werden, müssen digitale Identitäten bestmöglich geschützt werden. Dies ist besonders in der Industrie wichtig, denn hier kommunizieren Maschinen direkt miteinander, um automatisiert arbeiten zu können. Sie verteilen anfallende Aufgaben eigenständig über ihnen zugewiesenen Rechte. Darüber hinaus kommunizieren sie zum Beispiel mit ERP- oder MES-Systemen. Um einen reibungslosen Ablauf zu gewährleisten, müssen die Geräte sich deshalb nicht nur erkennen, sondern sich vertrauen können.

### Vertrauen ist gut, Kontrolle ist besser

Ein erster Schritt, eIDs zu schützen, ist zu kontrollieren, welche Maschinenidentitäten im Firmennetz genutzt werden und welche externen Geräte (z.B. von Mitarbeitern im Homeoffice) damit verbunden sind. Alle Geräte, die Zugriff auf das Netzwerk haben, sollten hinsichtlich der Sicherheitsupdates immer auf dem neuesten Stand sein, um keine Angriffsfläche für Cyberkriminelle zu bieten. Und möglichst kryptische Passwörter sind schwerer zu hacken.

Der wichtigste Schritt ist aber die zweifelsfreie Identitätsfeststellung. Sie kann zum Beispiel über x.509 Zertifikate erfolgen, die zur Identitätsüberprüfung und Übertragung verschlüsselter Daten verwendet werden. Sie dienen als sichere Kennungen und digitale Pässe, die Informationen über den Besitzer tragen. Ihre Vertrauenswürdigkeit wird durch eine autorisierte Zertifizierungsstelle (CA) gewährleistet.

Bei der Verwaltung der stetig wachsenden Zahl an Zertifikaten im Unternehmen helfen Zertifikatemanager wie der essendi xc. Er ermöglicht die Übersicht und Kontrolle der im Unternehmen befindlichen Zertifikate hinsichtlich Anzahl, Ablaufdaten und Installationsorte.

Wir bei essendi it entwickeln IT-Lösungen für Finanzdienstleister, Handel und Industrie auf aktuellem technologischem Niveau. Dabei sind wir spezialisiert auf IT-Sicherheit und Zertifikatemanagement.

essendi it
IT-Beratung und -Entwicklung

**essendi it GmbH**
Dolanallee 19
74523 Schwäbisch Hall
Telefon 07 91-94 30 70-12
Internet: www.essendi.de