DTS IDENTITY CLIENT

Der "Endpunkt" ist für jeden Hacker Gold wert, weil wir von Endgeräten umgeben sind. Die Anzahl der vernetzten Devices geht in die Milliarden, Tendenz steigend, teilweise jedoch veraltet und abhängig von der Bedienung des Benutzers. 88% aller Datenschutzverletzungen werden durch menschliches Versagen verursacht. Wenn Unternehmen nicht sicherstellen, dass jedes Gerät, welches Zugriff auf interne Ressourcen erhält, auch die Sicherheitsrichtlinien erfüllt, kann es kein besseres Einfallstor geben. DTS Identity ist DIE Plattform für alle Identitäten. Mit dem DTS Identity Client härten wir die Lösung nun zusätzlich und ermöglichen ECHTE Zero-Trust-Identity.

WAS IST DER "CLIENT" FÜR UNSER DTS IDENTITY?

Der DTS Identity Client ist keine einzelne Lösung, sondern knüpft direkt an das DTS Identity IAM an. Er ermöglicht es, nicht nur den User zu identifizieren und zu authentifizieren, sondern auch das dazugehörige Device und dessen Zustand als wichtigen Faktor miteinzubeziehen. Gleichzeitig können wir die Features des DTS Identity auf Clients erweitern. Somit bekommt unser eigenentwickeltes Identity & Access Management einen größeren Hebel für die Umsetzung einer Zero-Trust-Strategie.
Um sicherzustellen, dass durchgehend die neuste Version zur Verfügung steht, wird die Lösung ausschließlich „as a Service" angeboten. So kann der DTS Identity Client ohne internen Aufwand genutzt werden und ohne sich um das Hosting Gedanken machen zu müssen. Natürlich wird die Gesamtlösung nur aus unseren deutschen, zertifizierten Rechenzentren bereitgestellt.

FEATURES & DEREN VORTEILE

1. TRANSPARENZ

- Sichtbarkeit aller Devices im Netzwerk
- Status der Devices auf einen Klick einsehbar
- Übersicht, wie viele & wann Devices auf Unternehmens-Apps zugreifen
- Mehr Transparenz ermöglicht mehr Regelwerke

2. REGELSETZUNG

- Aufsetzen individueller oder universaler Endpunkt- & MFA-Richtlinien
- Regelsetzung von Compliance-Richtlinien geschieht zentral im DTS Identity durch unser Conditional Access Feature
- Use Case Beispiel: Laut Compliance-Richtlinie soll nur mit sicheren Devices auf Unternehmens-Apps zugegriffen werden können. Die Devices benötigen eine aktuelle Version des Betriebssystems und notwendige Sicherheiten, z. B. einen aktiven Firewall- und/oder Antivirus-Status. Erst wenn dies sichergestellt ist, wird ein Zugang zu (wichtigen) Anwendungen ermöglicht.

3. DURCHSETZUNG DER REGELUNGEN BZW. AUDIT & LOGS

- Nachverfolgung & Belegung von Compliance-Richtlinien
- Durch Transparenz von Logs kann direkt eingesehen werden, welche Clients in welcher Form aktiv sind/waren & weshalb
- Gut einsetzbar für Audits & Compliance-Dokumentation

4. KOMBINATION VON NETZWERK-, DEVICE- & IDENTITÄTENSICHERHEIT

- Optimale Verknüpfung der Sicherung des Netzwerks, der jeweiligen Devices & der Identitäten:
  - DTS Identity: Anmeldung, MFA & Conditional Access (Durchsetzung der Richtlinien)
  - DTS Identity Client: Sichtbarkeit des Devices & des jeweiligen Device-Zustands
  - ARP-GUARD NAC: Sicherung des Netzwerks

DTS Systeme GmbH
+49 5221 1013-000

DTS Systeme Münster GmbH
+49 251 6060-0

dts.de
info@dts.de