

WEBSERVER & ROUTER

MIT BRIEF UND SIEGEL IM NETZ

Je weiter die Digitalisierung voranschreitet, desto größer wird die Bedeutung von Online-Diensten und -Services für die Wirtschaft. Gleichzeitig nimmt die Zahl der Cyber-Angriffe immer weiter zu – und das in rasantem Tempo.

In Sachen IT-Security gilt es also aufzurüsten:

- Kundendaten bei der Nutzung der Website schützen.
- Vertrauliche Firmendaten innerhalb des Netzwerkes schützen.
- Remote-Zugänge gegen Unberechtigte und Datenverlust schützen.

BEISPIELE

RISIKEN FÜR HANDEL

Manipulation von Bestellungen und Ausschreibungsunterlagen.
Verunsicherung der B2B Partner. Imageverlust.

RISIKEN FÜR FERTIGUNG

Verlust von Betriebsgeheimnissen.
Maschinenausfälle durch Datenmanipulation.
Industriespionage.

RISIKEN FÜR DIENSTLEISTUNG

Ausspähung von Kundendaten und Identitätsklau drohen.
Datenschutzvorgaben werden verletzt.
Vertrauensverlust / Umsatzeinbruch drohen.



MÖGLICHE GEFAHREN

- Gezielte Cyberangriffe auf vertrauliche Unternehmens- und Kundendaten.
- Datenschutzvorgaben werden nicht erfüllt, weil die Kommunikation über unsichere elektronische Kanäle erfolgt.
- Missbrauch der Unternehmenspräsenz / Kundenkommunikation durch Phishing.



DIE LÖSUNG

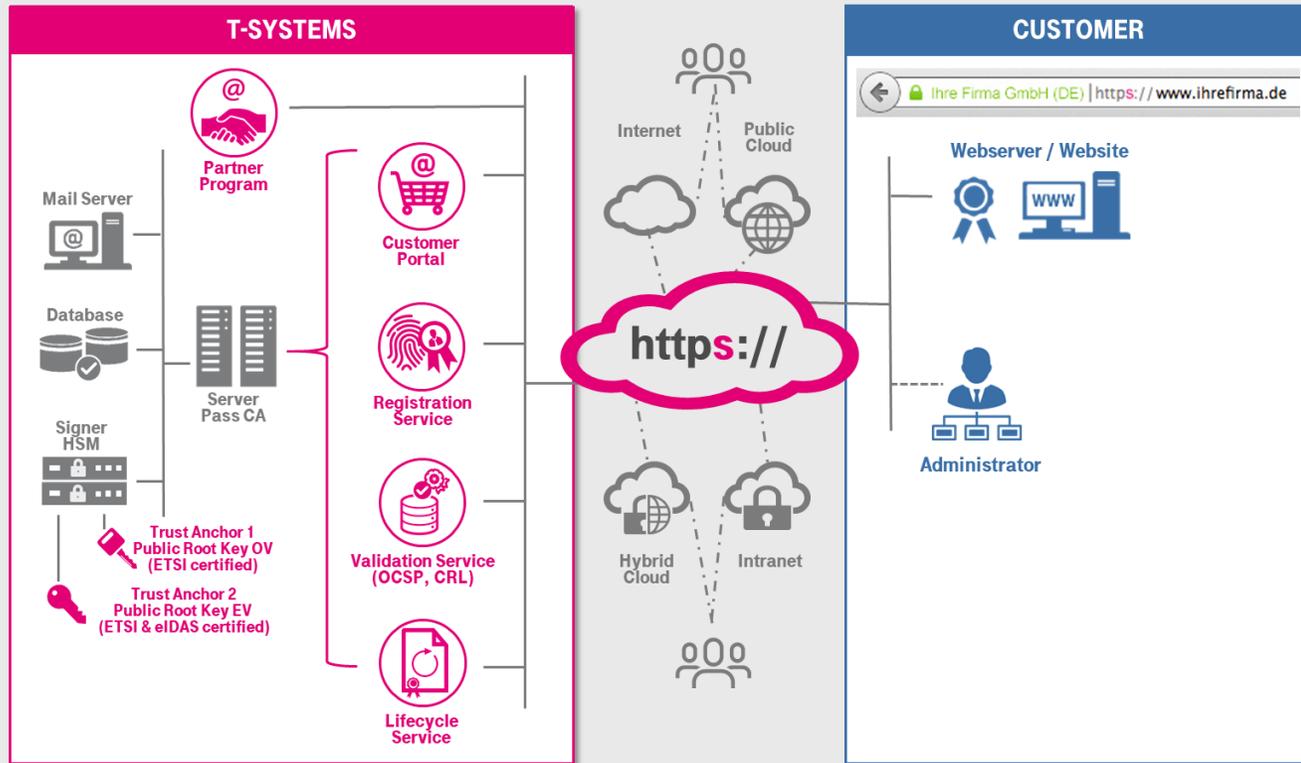
Die Server.ID, der digitale Ausweis für Ihren Server. SSL-Zertifikate (Secure Sockets Layer; auch TLS-Zertifikate genannt (Transport Layer Security)) sind hier ein elementarer Bestandteil. Sie sorgen für Sicherheit beim Datentransport und schaffen eine Vertrauensbasis.



SERVER.ID

VORTEILE AUF EINEN BLICK

- 🔒 Zertifikate unterstützen neueste TLS-/SSL-Standards.
- 🔒 Schutz vor Daten- und Knowhow-Missbrauch.
- 🔒 Absicherung gegen finanzielle Schäden – z.B. durch Datenklau und Imageverlust.
- 🔒 Abschreckung von Cyber-Kriminellen u. Industriespionen.
- 🔒 Verhinderung von Online-Kaufabbrüchen.
- 🔒 Sicherheitsindikator (grüne Adressleiste, Schlosssymbol) im Browser.
- 🔒 Plattformentwicklung in Deutschland; Betrieb im Telekom Trust Center in Deutschland.
- 🔒 Zertifiziert nach ETSI; konform zu den Vorgaben des CA/Browser Forums.
- 🔒 Zertifikate „Made in Germany“. eIDAS konform (nur EV).



LEISTUNGEN: Standard

inkl. Firmendaten
1 Domaineintrag.

Erweiterung Wildcard

Beliebig viele Subdomains einer Ebene.

Erweiterung SAN

Multidomain Zertifikat für mehrere Domains.



Extended Validation

inkl. **erweiterte** Firmendaten
1 Domainname.

Nach den strengen Vergaberichtlinien des CA/Browser Forums.

Erweiterung SAN

Multidomain Zertifikat für mehrere Domains.

Allgemeines

- Laufzeiten 1 Jahr
- SHA256 / Schlüssel-längen > oder = 2048 Bit.
- Von allen aktuellen Browsern als vertrauenswürdig eingestuft.
- **Partnerprogramm.**

INTERESSE?

Vertrauen Sie dem führenden Anbieter von Sicherheitslösungen.

Kontakt:

Deutsche Telekom Security GmbH
Telesec_Support@t-systems.com
www.telesec.de

