Website-Zertifikate

Was Sie über SSL-Zertifikate wissen müssen

Drei Hauptgründe für Website-Zertifikate

SICHERHEIT

Die Daten Ihrer Website werden verschlüsselt übertragen. So schützen Sie die **sensiblen Daten** Ihrer Kunden. Besonders für User-Eingaben etwa bei Formularen ist das sehr wichtig.

VERTRAUEN

Das SSL-Protokoll schafft Vertrauen in Ihre Website und damit in Ihr Unternehmen. Je nach **Zertifikatstyp** werden die Unternehmensdaten bei Antragsstellung von vertrauenswürdiger Zertifizierungsstelle geprüft.

RANKING

Ein SSL-Zertifikat kann die Platzierung Ihrer Seite in der **Suchmaschine** verbessern. Seit 2014 sind SSL-Zertifikate ein Ranking-Kriterium bei Google.

Welcher Zertifikatstyp ist für welche Website empfehlenswert?

DV-SSL	OV-SSL	EV-SSL
Domain Validation	**Organisation Validation**	**Extended Validation**
Die Zertifizierungsstelle prüft, ob der Auftraggeber auch Inhaber der Domain ist.	Zusätzlich zum Domaincheck findet eine Identitätsprüfung der beantragenden Organisation statt.	Neben Domaincheck und Organisationsvalidierung ist ein individueller Identitätsnachweis vorgesehen.
https:// und grünes Schlosssymbol	https:// und grünes Schlosssymbol	https:// und grünes Schlosssymbol
Domaincheck	Domaincheck	Domaincheck
	Identitätsprüfung der Organisation	Erweiterte Identitätsprüfung und Legitimation des Antrags
Keine Identitätsprüfung! Gefahr von Phishing-Angriffen und Datenmissbrauch		**QWAC (Qualified Website Authentication Certificates)** nach eIDAS mit hoher Rechtsverbindlichkeit
BLOGS UND COMMUNITIES	**UNTERNEHMEN UND ORGANISATIONEN**	**ONLINE-SHOPS, BANKEN UND FINANZBRANCHE**

Allein im April 2018 hat die Webseite **Phishbank.org** über 3.200 Webseiten identifiziert, die für Datenmissbrauch genutzt wurden. Von diesen hatten 99 Prozent DV-Zertifikate im Einsatz.

BUNDESDRUCKEREI