FILEBOX*local*

... all in one box

FILEBOX

- Datenempfang - ***kompatibel***
- Auftragsmanagement - ***übersichtlich***
- Jobtickets - ***präzise***
- Datenversand - ***unlimitiert***
- Fileserver - ***universell***
- E-Mailserver - ***spamfrei***
- Fax, Bilddatenbank, e.t.c. - ***optional***

>> FILEBOX – the digital courier

- schnell
- zuverlässig
- sicher
- einfach

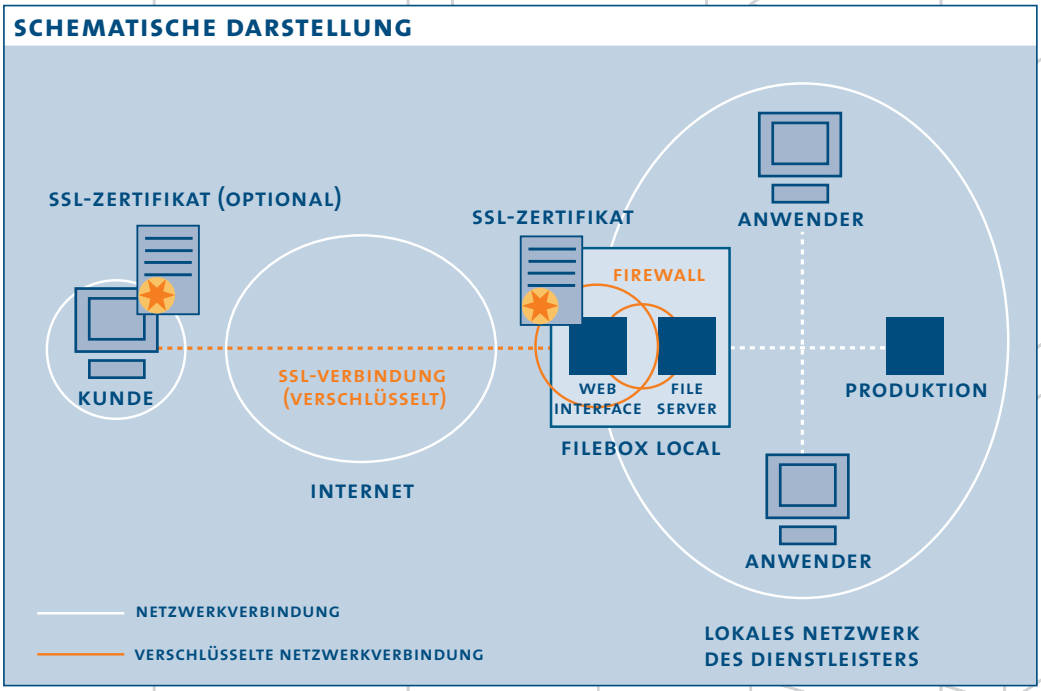
Sicherheitskonzept

DATENSICHERHEIT BEI HTTP(S)-DATENTRANSFER

FILEBOXlocal bietet Ihnen eine umfassendes Konzept zur Gewährleistung einer sicheren Datenübertragung zwischen Ihren Kunden und Ihrer Druckvorstufe.
Das Konzept beinhaltet folgende Faktoren:

- Eindeutige Identifizierung des Servers über ein offizielles Sicherheitszertifikat
- optional ist die zusätzliche Identifizierung des Senders über ein Zertifikat möglich
- Verschlüsselung der Datenübertragung per SSL mit 128 bit Verschlüsselung
- Authentifizierung des Senders per Passwort am Server
- Zeitsperre bei Eingabe falscher Passwörter
- Absicherung des Servers per Firewall zur Unterbindung unbefugter Zugriffe
- Verschlüsselung der Dateinamen auf dem Server
- Dateizugriff auf Kundendateien ausschließlich aus dem Kundennetzwerk möglich
- Vollständiger Schutz der auf dem Server abgelegten Daten vor Zugriffen aus dem Internet
- Zusätzliche Möglichkeit der automatischen Löschung eingegangener Daten vom Webserver direkt nach Dateieingang. (Daten werden automatisch auf den integrierten Fileserver übertragen) Der Zugriff auf den Fileserver ist nur über das Kundennetzwerk möglich.
- Physikalische Trennung des externen und internen Netzwerkes durch separate Netzwerkschnittstellen.

SCHEMATISCHE DARSTELLUNG



ERLÄUTERUNGEN

Was ist SSL-Verschlüsselung?

SSL (Secure Socket Layer) bezeichnet ein Verfahren zur Verschlüsselung, durch das unberechtigte Dritte am Lesen im Internet übermittelter Daten gehindert werden. Es wurde von Netscape eingeführt und hat sich mittlerweile als Standard etabliert. Nach der Verbindungsaufnahme mit dem Webserver einigen sich beide Seiten (Browser und Webserver) auf einen sogenannten Sitzungs-Schlüssel.

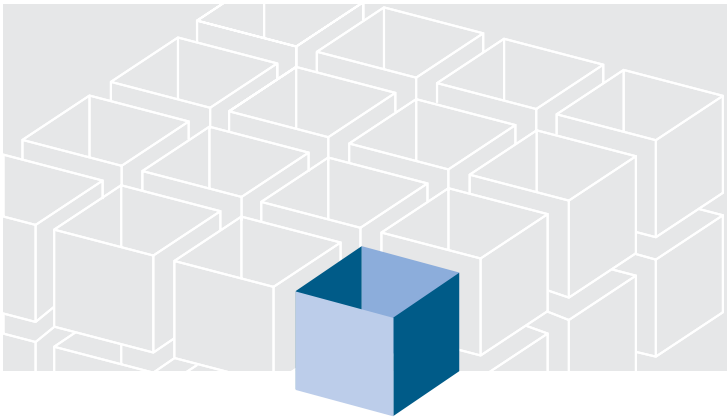
Nach diesem Vorgang wird die Kommunikation zwischen beiden Partnern mit dem Sitzungs-Schlüssel verschlüsselt. Die Verschlüsselung wird im Protokoll in der Regel als https:// angegeben. Sie ist oft auch in der unteren Leiste des Browserfensters an einem kleinen Symbol (zum Beispiel einem Vorhängeschloss) zu erkennen. Derzeit dürfen in Deutschland Daten mit maximal 128Bit verschlüsselt werden.

Warum Sicherheitszertifikate?

Zur Etablierung einer SSL-Verbindung ist ein Sicherheitszertifikat erforderlich. Sicherheitszertifikate von offiziell anerkannten Instituten wie z.B. Verisign oder Thawte bestätigen dabei die Authentizität des Servers. Der Internetnutzer kann somit zweifelsfrei feststellen, daß der Server, mit dem Kontakt aufgenommen wird nicht gefälscht wird. Hiermit wird das sog. “Phishing” (fälschen einer Serveradresse mit dem Zweck der Umleitung des Nutzers) unterbunden. Bei bewußter Benutzung ist es also unmöglich, daß die Daten an eine gefälschte Adresse gelangen.
Das SSL-Zertifikat enthält Informationen über den Aussteller, die Firma und den Server. Es kann von jedem Nutzer zur Überprüfung eingesehen werden, bevor eine Verbindung zum Server aufgenommen wird.
Im umgekehrte Fall kann der Server bei Verwendung eines Client-Zertifikates automatisch überprüfen, ob der Sender berechtigt ist. Unberechtigte Sendungsversuche werden damit von vornherein unterbunden.

SPEZIFISCHE ANPASSUNGEN

Wir sind offen für Anpassungen an spezielle Anforderungen an Ihre firmeninternen Sicherheitsstandards. Bitte sprechen Sie uns einfach an. Wir erörten gerne mögliche Anpasungen unserer Sicherheitsfeatures in einem persönlichen Gespräch.



FILEBOX

kontakt:
base-t GmbH & Co. KG
Max-Keith-Str. 11
d-45136 Essen
Germany
phone: +49-201-2667083
fax: +49-201-2667084
e-mail: service@filebox.de
web: www.filebox.info