CryptoWeb für Web-Portale und Web-Anwendungen

Was ist CryptoWeb?

Bei *CryptoWeb* handelt es sich um ein System, welches Sie als Modul in Ihre Web-Installation einbinden können. Durch die Vergabe und Überprüfung von Client-Zertifikaten mittels CryptoWeb sind ausschließlich autorisierte Zugriffe auf ihre Anwendung möglich. CryptoWeb nutzt hierfür ausschließlich in allen Webbrowsern fest integrierte Funktionen und benötigt keine weitere Software oder Plug-Ins auf den Client-Rechnern.

Warum benötigt Ihr Unternehmen CryptoWeb?

Sie vertrauen ihrer Anwendung tagtäglich hochsensible Informationen aus allen Gebieten eines Kunden an. Ein Zugriff auf diese Daten durch unberechtigte Personen kann zu erheblichen Schäden sowie zu einem massiven Vertrauensverlust bei Ihren Kunden führen.

Ohne CryptoWeb ist Ihre Web-Installation von allen Teilnehmern im Internet erreichbar und somit grundsätzlich angreifbar. CryptoWeb kann dieses Risiko erheblich reduzieren, indem nur zweifelsfrei identifizierten Teilnehmern der Zugriff auf ihre Anwendung gestattet wird.

Wie funktioniert CryptoWeb im Detail?

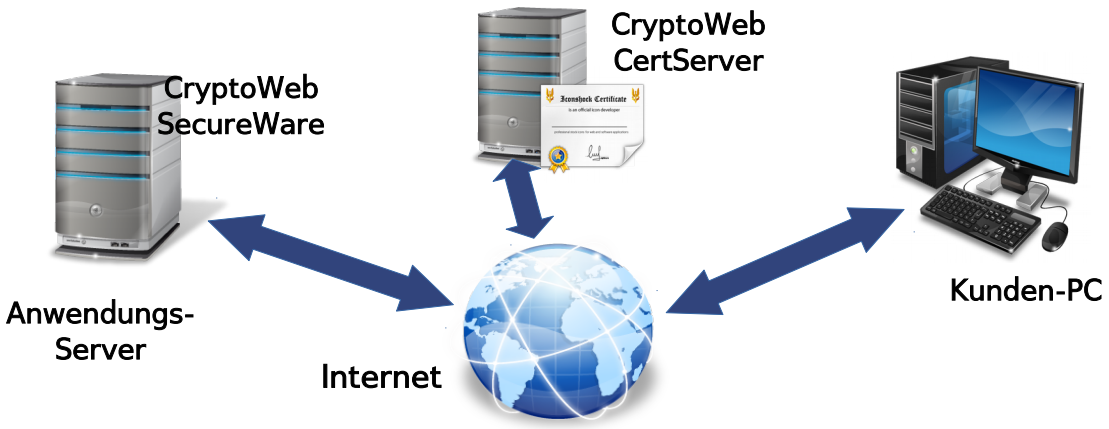
Nach der Installation und Einrichtung von CryptoWeb arbeitet CryptoWeb wie ein Schutzschild vor ihrer Anwendung, und lässt nur noch Anfragen von Browsern passieren die mit einem gültigen Zertifikat ausgestattet sind. Die Ausstellung und Verwaltung der Zertifikate übernimmt dabei der CryptoWeb CertServer. Die Überprüfung und Weiterleitung von Anfragen ist Aufgabe der CryptoWeb SecureWare.

Zertifikatsdeployment über einen zweiten Übertragungsweg oder ein Post-Clearing-Verfahren

Ein zweiter Übertragungsweg kann z.B. die Handynummer des Endanwenders sein. Dieser bekommt dann per SMS eine TAN übermittelt. Nach Eingabe der TAN während der einmaligen Zertifizierung wird das Zertifikat ausgestellt.

Beim Post-Clearing wird der Browser beim ersten Zugriffsversuch auf ihre Anwendung mit einem gültigen jedoch noch nicht freigeschalteten Zertifikat versorgt, und im selben Schritt eine eindeutige Identifikationsnummer angezeigt. Im Anschluss muss der Endanwender beim Administrator eine Freischaltung dieses Zertifikats beantragen. Ein Zugriff auf ihre Anwendung ist erst nach dieser Freischaltung möglich. Im Rahmen des Post-Clearing-Verfahrens kann, statt der eindeutigen Identifikationsnummer vom Endanwender, auch die Angabe des Client-Zertifikat-Fingerprints verlangt werden. Durch diese manuelle Überprüfung des Zertifikat-Fingerprints kann ein Man-in-the-middle-Angriff noch sicherer ausgeschlossen werden.

CryptoWeb - Technische Umsetzung



CryptoWeb für Web-Portale und Web-Anwendungen

Ihre Vorteile bei der Nutzung von CryptoWeb:

Security

Für jeden Benutzer gibt es immer nur ein gültiges Zertifikat. Die missbräuchliche Nutzung wird dadurch sicher erkannt.

Usability

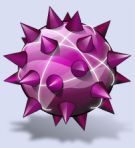
Da jede von CryptoWeb SecureWare weitergeleitete Anfrage die Zertifikatsdaten enthält, können Sie diese Daten zum LogIn nutzen. Der Enduser benötigt also kein Passwort mehr und ist dennoch sicher identifiziert.

Sichere Zertifikatsausstellung

Die Freischaltung neuer Zertifikate erfolgt nach Ihren Wünschen:
Über einen zweiten Übertragungsweg (Handynummer → SMS → TAN → Zertifikat)
Oder im Post-Clearing-Verfahren durch einen Administrator. Die Freischaltung kann über eine alphanumerische ID oder über den Zertifikats-Fingerprint entsprechend Ihres Sicherheitsbedürfnisses erfolgen.
In jedem Fall wird die Identität des Benutzers sicher festgestellt.

Zyklischer Zertifikatstausch

Die Zertifikate, welche PC-Arbeitsplätze gegenüber ihrem Anwendungs-Server identifizieren werden automatisch regelmäßig ausgetauscht. So können Sie sicher sein, dass selbst wenn Zertifikate verloren gehen sollten, diese zeitnah ungültig werden. Den Tauschzyklus können Sie entsprechend Ihres Sicherheitsbedürfnisses frei wählen.



Reduzierte Angriffsvektoren

Auf ihrem Anwendungs-Server können zukünftig nur noch Rechner mit einem gültigen CryptoWeb-Zertifikat zugreifen. Auf diesem Weg wird die Zahl aller potentiellen Angreifer auf bekannte Personen reduziert. Selbst Mitarbeiter, die über ein gültiges Benutzerkonto verfügen, können nur über freigeschaltete Arbeitsstationen auf ihre Anwendung zugreifen.

Schutz vor DoS-Attacken

Ihr Anwendungs-Server ist aus dem Internet nicht mehr direkt erreichbar, somit kann dieser auch kein Ziel von DoS-Angriffen werden da alle unberechtigten Anfragen bereits auf der Ebene von CryptoWeb blockiert werden. Durch Bereitstellung zusätzlicher Ressourcen für CryptoWeb ist es einfach möglich, die Leistungsfähigkeit dieser Schutzschicht zu skalieren um einem Angriff zu begegnen und ihre Anwendung weiterhin verfügbar zu halten. Ihre Anwendung im selben Maße zu skalieren ist kaum möglich.