

Sicherer Datentransfer zwischen Bürger, Formularserver & Verwaltung.

E-Government – Aber sicher!

Für integriertes E-Government müssen sich interne Verfahren nach außen öffnen. Jede weitere Öffnung stellt jedoch auch immer ein zusätzliches Sicherheitsrisiko dar. Um den stets steigenden Anforderungen gerecht zu werden aber auch Schadsoftware frühzeitig zu erkennen und effektiv zu beseitigen, ist der Einsatz eines Sicherheitssystems unabdingbar.

Mit dem Form-Solutions-Security-Paket bieten wir Ihnen den sicheren Datenaustausch zwischen Antragsmanagement, Verwaltung und Bürger:in. Neben dem klassischen **Virens Scanner** setzen wir auf den **SecureConnector** und das Sicherheits-Framework **Fail2Ban**.

Virens Scanner
SecureConnector
Fail2Ban

Virens Scanner

Anlagen sind ein wichtiger Bestandteil von Antrags- und Bestellprozessen. Um bereits beim Ausfüllprozess zu gewährleisten, dass durch den Upload von Anlagen Bürger*innen keine Schadsoftware übergeben können, enthält das Security-Paket einen Virens Scanner.

Noch vor dem eigentlichen Serverupload durchleuchtet der Virens Scanner die Dateien auf Schadsoftware. Ist die Datei verdächtig und zeigt Anzeichen auf Viren, Würmer, Trojaner oder andere Malware, wird der Upload verweigert.



Hinweis:

Für die Nutzung der Virens Scanner-Funktion ist keine zusätzliche Installation notwendig. Sie kann sofort bei den bestehenden sowie neuen Antragsassistenten und PDF-Formularen verwendet werden.

Fail2Ban

Das Sicherheits-Framework Fail2Ban ist ein Modul, welches DDoS-Attacken verschiedenster Art unterbindet. Hierzu wird mit Hilfe eines Logfiles der Server überwacht und nach IP-Adressen durchsucht, die ein ungewöhnliches Verhalten aufweisen. So können IP-Adressen, z.B. anhand einer festgelegten Anzahl von Einreichungen der Antragsassistenten bzw. PDF innerhalb eines definierten Zeitraums temporär gebannt bzw. blockiert werden.



Hinweis:

Für die Nutzung des Fail2Ban ist keine weitere Installation erforderlich.



SecureConnector

Der Form-Solutions-SecureConnector ermöglicht es, Fachverfahren in einer geschützten, vom Internet getrennten IT-Landschaft zu betreiben und gleichzeitig eine komfortable Integration zum Formularserver zu nutzen. Der SecureConnector wird dafür im geschützten Bereich (DMZ) installiert sowie ein „Kommunikationskanal“ zum Formularserver geöffnet.

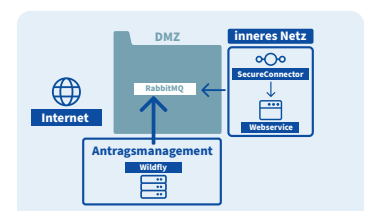
„SecureConnector“- Variante 01

Der SecureConnector wird im internen Netz und die RabbitMQ in der DMZ des Fachverfahrens installiert und kommunizieren mit dem Formularserver.

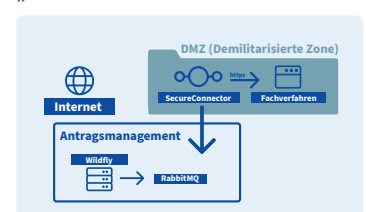
„SecureConnector“- Variante 02

Der SecureConnector wird in der DMZ installiert und kommuniziert mit der RabbitMQ des Formularservers.

„SecureConnector“- Variante 01



„SecureConnector“- Variante 02





FACEBOOK

INSTAGRAM

YOUTUBE

TWITTER

XING



FORM-SOLUTIONS GMBH

Bahnhofstraße 10
76137 Karlsruhe

Tel.: +49 721 754055-0
Fax: +49 721 754055-717

E-Mail: info@form-solutions.de

www.form-solutions.de