



# Website- Sicherheitsanalyse

## Sicherer Auftritt im WWW.

Weltweit greifen 2,5 Milliarden Nutzer auf knapp 700 Millionen Webseiten zu. Ob Informationsplattform, E-Shop oder Dienstleistungsportal: Mit einer professionellen Website-Sicherheitsanalyse Ihrer Internetpräsenz machen Sie Ihren Internetauftritt zu einem Gewinn für Kunden, Interessenten, Partner und nicht zuletzt Ihr Unternehmen oder Ihre Organisation.

### Ihre Internetpräsenz unter Beschuss

Webserver gehören zu den am häufigsten attackierten Systemen im Internet. Kein Wunder: Komplexe Konfiguration und funktionsreiche Web-Applikationen machen sie anfällig für Sicherheitslücken. Zudem sind Webserver Tag und Nacht online. Kriminelle unterschiedlicher Motivation haben viel Zeit, um auch kleinste Schwachstellen zu entdecken. Vom „Defacement“ (Umleitung zu einer Fremdpräsenz) über den Abfluss vertraulicher Daten bis hin zur Schadcode-Verteilung in Ihrem Namen reicht die Spanne drohender Risiken.

### Auf einen Blick:

- › Systematische Durchsicht der Präsenz entsprechend WASC Threat Classification (Liste der Bedrohungen für Web-Anwendungen des Web Application Security Consortium)
- › Einbeziehung sämtlicher relevanter Bedrohungen ohne Rücksicht auf Verbreitung oder Häufigkeit
- › Black-Box-Tests (Penetrationstests) und White-Box-Tests (Betrachtung von Funktion und Implementierung)
- › Effiziente Vorgehensweise durch werkzeuggestützte Verfahren in Kombination mit manueller Prüftechnik
- › Aussagekräftige, individuelle Analysenberichte, zielgruppenspezifische Präsentation durch Experten auf Wunsch
- › Konkrete, priorisierte Handlungsempfehlungen
- › Koordination externer Dienstleister, Nachprüfungen



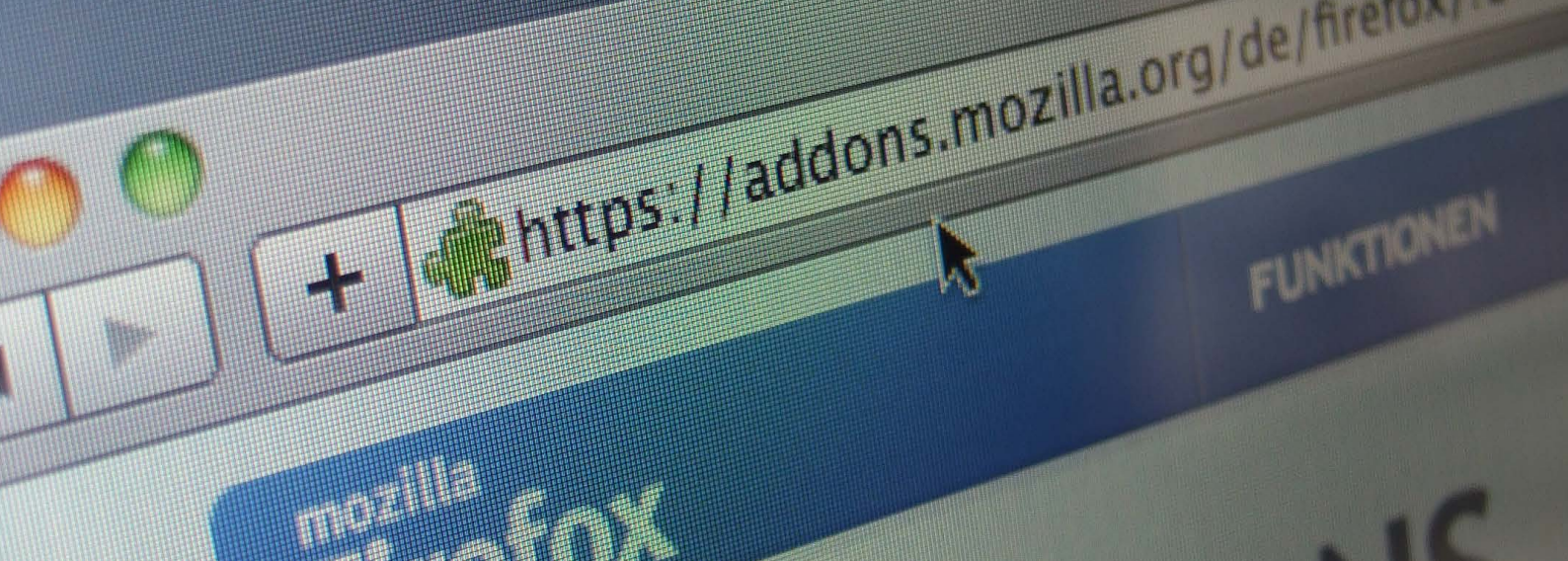
### Horrorszenario Webserver-Ausfall

Ein Online-Shop verweigert den Dialog, das Bürgerportal ist unerreichbar, die Fahrplanauskunft beantwortet keine Anfragen: ein Alptraum und Realität nach einem Webserver-Angriff. Bis die Ursache behoben ist, können durch die Ausfallzeit hohe Schäden entstehen. Beugen Sie vor.

### Gefahren erkennen - Lücken schließen

Die Konsequenzen eines Angriffs auf einen Webserver umfassen regelmäßig Reputationsverlust und wirtschaftliche Nachteile. Gute Gründe also, die eigene Website von Fachleuten im Hinblick auf IT-Sicherheit „auf Herz und Nieren“ prüfen zu lassen. So sparen Sie Zeit und Geld.

Website-Sicherheitsanalysen können Havarien und Ausfällen vorbeugen. Erkannte Sicherheitslücken können gezielt beseitigt und durch Angriffe nicht mehr ausgenutzt werden. Website-Sicherheitsanalysen sind eine nachhaltige Investition.



### Website-Sicherheitsanalyse - unsere Leistungen:

Voranalyse zur Eingrenzung der weiteren Untersuchung auf potenziell gefährdete Bereiche

Prüfung von Produktivsystemen ohne Dienstunterbrechung oder im Vorfeld der Betriebsaufnahme (z. B. bei Relaunch)

Handlungsempfehlungen mit Priorisierung nach Gefährdungspotenzial des zu neutralisierenden Angriffsvektors

Kosteneffiziente Vorgehensweise durch werkzeuggestützte Analyse in Kombination mit manueller Prüftechnik

Unterstützung bei der Erstellung von Pflichtenheften im Vorfeld notwendiger Verbesserungsmaßnahmen

Gefährdungsprognose im Fall von Kombinationsangriffen, auch für selten vorkommende Szenarien

Integrierte Betrachtung von Datenschutzaspekten und IT-Sicherheit für höchstmögliches Schutzniveau

### Im Blickpunkt: E-Business und E-Government

Millionen Menschen erledigen ihre Einkäufe online. Bürgerinnen und Bürger nutzen gern die stetig ausgebauten Internetangebote von Behörden und Verwaltungseinrichtungen. Webserver verarbeiten erhebliche Mengen sensibler Daten; eine Kompromittierung wäre ebenso fatal wie ein Ausfall. Web-Anwendungen zeichnen sich durch einen hohen Interaktionsgrad aus - aktive Inhalte sind an der Tagesordnung. Die bestehende Gefährdung kann durch eine systematische Website-Sicherheitsanalyse festgestellt werden.

**Testen Sie uns:** Wir untersuchen Ihre Internetpräsenz zunächst orientierend. Ergeben sich hierbei keine nennenswerten Beanstandungen, können Sie von Ihrem Analyseauftrag ohne weitere Verpflichtung zurücktreten.



### Wir können viel für Sie tun. Unsere weiteren Dienstleistungen:

- › Datenschutz-Erstanalyse
- › Stellung externer Datenschutzbeauftragter
- › Audit nach ISO 27001 (nativ und auf der Basis von IT-Grundschutz)
- › IS-Kurzrevision im Vorfeld eines Audits
- › Risikoanalyse, u. a. nach der Attack-Tree-Methode
- › Begleitende Beratung zu generellen Fragestellungen der IT-Sicherheit und des betrieblichen Datenschutzes

### Ihr Experte für IT-Sicherheit und Datenschutz:

**Roman Maczkowsky** ist zertifizierter Teamleiter für Audits nach ISO 27001 nativ sowie auf der Basis von IT-Grundschutz. Er ist ausgewiesener Spezialist in Sachen betrieblicher Datenschutz und war unter anderem Mitarbeiter des Unabhängigen Landeszentrums für Datenschutz Schleswig-Holstein (ULD) sowie des Berliner Beauftragten für Datenschutz und Informationsfreiheit. Roman Maczkowsky ist BSI-lizenziertes IS-Revisor sowie IS-Berater und als Referent in der Ausbildung von Datenschutz- bzw. IT-Sicherheitsbeauftragten tätig.

