# BASIS SECURITY CHECK
## FÜR SICHERE WEBANWENDUNGEN

**STARTERKIT - WEB SECURITY**

### GEHEN SIE KEIN RISIKO EIN.

**Im Rahmen des Basis Security Check werden Ihre Webanwendungen innerhalb von 3-5 Projekttagen aus der Position eines potentiellen Angreifers auf vorhandene Schwachstellen geprüft. Die Prüfergebnisse sind die Grundlage für eine erste Einschätzung des Sicherheitsniveaus Ihrer individuellen Anwendung.**

### WIE SICHER SIND SIE, DASS IHRE WEBSEITE SICHER IST?

Spektakuläre Hacker-Attacken sorgen immer wieder für viel Aufsehen. Politische Webseiten, die plötzlich die Thesen der Gegenseite verkünden oder gestohlene Kreditkartendaten von Touristen aus dem Datenzentrum eines großen Reiseveranstalters. Solche Einzelaktionen werden oft medienwirksam in Szene gesetzt.

Der größte Teil aller Hacker-Angriffe sind kriminell motiviert, um Unternehmensgeheimnisse aufzuspüren, Konten zu räumen oder personenbezogene Daten zu stehlen. Ist Ihre Web-Infrastruktur auf solche Situationen vorbereitet? Angriffe passieren unterwartet und ohne Vorwarnung. Werden sensible Daten gehackt kann das unangenehme juristische Folgen haben.

Um Sicherheitslücken zu erkennen bedarf es langjähriger Erfahrung zu Testmethoden und ein umfangreiches und aktuelles Know-How zu möglichen Angriffsszenarien.

### DAS TEST AND INTEGRATION CENTER...

von T-Systems Multimedia Solutions ist das derzeit einzige, von der Deutschen Akkreditierungsstelle anerkannte, Prüflabor der Internet- und Multimediabranche in Deutschland.

Mit über 175 ISTQB-zertifizierten Testexperten und 45 Spezialisten für IT-Security und Datenschutz prüfen wir die Qualität und Sicherheit von Web-Applikationen.

T · · Systems ·

# DIE PHASEN DES BASIS SECURITY CHECKS:

## 1 ERSTE ANALYSE DES SICHERHEITSNIVEAUS IHRER ANWENDUNG

Das Ziel der Vorbereitungsphase ist die Festlegung des Testumfangs, der technischen und betrieblichen Rahmenbedingungen und des Testvorgehens beim Basis Security Check. Bei der Auswahl der Testszenarien und der Erstellung der Testfälle werden die Testrisiken besprochen sowie die Planung von Notfallmaßnahmen mit Ihnen abgestimmt.

## 2 PRÜFUNG DER ANWENDUNG AUF VORHANDENE

Mit Hilfe eines Schwachstellenscanners werden sowohl die Webanwendungen als auch die Konfiguration des Systems automatisch auf bekannte Schwachstellen untersucht. Zur Ausführung des Tests werden keine Änderungen an der Anwendung oder den Servern vorgenommen. Die Durchführung von aktiven Angriffsversuchen erfolgt mit manuellen Tests. Hierfür werden spezielle Testfälle ausgewählt. Der Tests kann sowohl im Intranet als auch im Internet erfolgen.

## 3 BESCHREIBUNG MÖGLICHER ANGRIFFSSZENARIEN UND DOKUMENTATION DER PRÜFERGEBNISSE

In dieser Phase des Checks werden die Prüfergebnisse bewertet sowie potenziell erfolgreiche Angriffsszenarien beschrieben. Die Präsentation der Ergebnisse erfolgt im Rahmen eines Abschlussworkshops.

## 4 EMPFEHLUNG VON MASSNAHMEN ZUR BESEITIGUNG DER SCHWACHSTELLEN

In Auswertung der Prüfergebnisse werden geeignete Maßnahmen zum Schließen der vorhandenen Schwachstellen definiert.

**STARTERKIT**
3 - 5 ROJEKTTAGE



**IHR ANSPRECHPARTNER**

Thomas Haase
Leiter Security and Data Privacy
Test and Integration Center

T-Systems Multimedia Solutions GmbH
Riesaer Straße 5, 01129 Dresden

Tel: +49 351 2820 2206
Mobil: +49 175 588 4475
E-Mail: t.haase@t-systems.com

www.tic-starterkits.de