

SECURITY CHECK INFRASTRUKTUR

BASIS CHECK FÜR EINE SICHERE IT-INFRASTRUKTUR



STARTERKIT - CYBER SECURITY

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 Millionen veröffentlichter Facebook-Profile. Solche Einzelaktionen werden oft medienwirksam von den Angreifern 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 Infrastruktur auf solche Situationen vorbereitet? Sind Ihre Netzwerkkomponenten wie Firewalls, Router und

Server sicher konfiguriert und ausreichend gehärtet? Um dies zu prüfen, werden im Rahmen des Infrastruktur Basis Security Checks Ihr Netzwerk und Ihre Systeme auf potentielle Schwachstellen untersucht und aufbauend auf den Ergebnissen Handlungsempfehlungen zur Absicherung Ihres Netzwerks gegeben.

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.

GEHEN SIE KEIN RISIKO EIN.

Im Rahmen des Basis Security Checks Infrastruktur werden Ihre Infrastruktur und Ihr Netzwerk innerhalb von 2 Projekttagen aus der Position eines potentiellen Angreifers auf vorhandene Schwachstellen geprüft. Die Prüfergebnisse dienen dem gezielten Auffinden von Schwachstellen in Ihrem Netzwerk und sind die Grundlage für eine erste Einschätzung des Sicherheitsniveaus Ihrer Infrastruktur. Im Rahmen der Auswertung der Prüfergebnisse werden geeignete Maßnahmen zum Schließen der vorhandenen Schwachstellen definiert.

DIE PHASEN DES BASIS SECURITY CHECKS:

1 ERSTE ANALYSE DES SICHERHEITSNIVEAUS IHRER INFRASTRUKTUR

Das Ziel der Vorbereitungsphase ist die Festlegung des Testumfangs, der technischen und betrieblichen Rahmenbedingungen und des Testvorgehens beim Basis Security Check Infrastruktur. Weiterhin werden mögliche Testrisiken besprochen sowie die Planung von Notfallmaßnahmen mit Ihnen abgestimmt. Zudem erfolgt eine Informationsbeschaffung hinsichtlich der zu prüfenden Systeme, IP Adressen, eingesetzten Dienste und Anwendungen.

2 PRÜFUNG DER INFRASTRUKTUR AUF VORHANDENE SCHWACHSTELLEN

Mit Hilfe eines Schwachstellenscanners untersuchen wir Ihr Netzwerk und die Systeme auf bekannte Schwachstellen. Im Rahmen dieses Scans werden Informationen über die Sicherheitsmerkmale Ihrer Systeme gesammelt und dokumentiert. Dadurch können offene Ports, kritische Dienste und weitere potentielle Sicherheitslücken identifiziert werden. Eine Änderung an Ihren Systemen erfolgt nicht. Die Durchführung der Tests kann sowohl im Intranet als auch im Internet erfolgen.

3 BESCHREIBUNG MÖGLICHER ANGRIFSSZENARIOEN UND DOKUMENTATION DER PRÜFERGEBNISSE

In dieser Phase des Checks werden die Prüfergebnisse bewertet, sowie potenziell erfolgreiche Angriffsszenarien beschrieben. Hierbei identifizieren wir Schwachstellen und Angriffsvektoren, die auch ein potentieller Angreifer finden und ausnutzen könnte.

4 EMPFEHLUNG VON MASSNAHMEN ZUR BESEITIGUNG DER SCHWACHSTELLEN

Im Rahmen der Auswertung der Prüfergebnisse werden geeignete Maßnahmen zum Schließen der vorhandenen Schwachstellen definiert. Die Präsentation der Ergebnisse erfolgt im Rahmen eines Abschlussworkshops.

STARTERKIT
3 - 5 PROJEKTTAGE

KONTAKT

Mitarbeiter Kontakt:

Thomas Haase

Tel: +49 351 2820 2206

Mobil: +49 175 5884 475

E-Mail: t.haase@t-systems.com

MMS Kontakt:

T-Systems Multimedia Solutions GmbH

Riesaer Straße 5

D-01129 Dresden

Tel.: +49 351 2820 0

www.t-systems-mms.com

www.test-and-integration.de