SICHERE ICT-SYSTEME – AUF HERZ UND NIEREN GEPRÜFT.

Mit Penetrationstests technische Schwachstellen identifizieren.

INTENSIV-CHECK SCHAFFT SICHERHEIT.

In Zeiten wachsender Cyber-Kriminalität ist es unverzichtbar, das Sicherheitsniveau der eigenen ICT-Infrastruktur realistisch einzuschätzen. Mit welchem Aufwand können Angreifer zum Beispiel über ein Webportal in die Backend-Systeme eindringen? Wie gut sind Kunden- und Geschäftsdaten geschützt? Um diese Fragen zu beantworten, müssen Systeme heute regelmäßig und sachgerecht überprüft werden. Bei einem Sicherheitstest führen Experten eine Bestandsaufnahme durch und durchleuchten systematisch den aktuellen Sicherheitsstand eines IT-Systems.

SICHERHEITSSTANDARDS ERFÜLLEN.

Für ein Risikomanagement, das ein realistisches Bild der System- und Anwendungssicherheit zeichnen will, sind Sicherheitstests unverzichtbar. Auch öffentliche Standards und Normen zum Beispiel des Bundesamts für Sicherheit in der Informationstechnik (BSI) schreiben regelmäßige Prüfungen und die Dokumentation von Schwachstellen vor.

CYBER-ANGRIFF IM KUNDENAUFTRAG.

Wer wissen will, wie stabil und sicher seine Systeme sind, muss letztlich die Methoden der Angreifer anwenden. Deshalb führt T-Systems mit so genannten Penetrationstests „Cyber-Attacken im Kundenauftrag“ durch. Indem sich Sicherheitsexperten in die Rolle von Angreifern versetzen und deren Denkweisen und Methoden übernehmen, können sie technische Schwachstellen am zuverlässigsten identifizieren, überprüfen und gezielte Gegenmaßnahmen ableiten.

NEUTRALER BLICK VON AUSSEN.

T-Systems verfügt als ICT-Dienstleister über die Expertise und die notwendige Unabhängigkeit, um den Sicherheitszustand der Systeme und Anwendungen kritisch zu analysieren. Haben Unternehmen bereits Tests und Prüfungen durchgeführt, baut T-Systems auf diesen Ergebnissen auf. Es wird großer Wert darauf gelegt, dass die Durchführung der Penetrationstests effizient und in klarer Abstimmung mit den Betriebsprozessen des Kunden erfolgt.

* Unverbindliche Preisangabe. Verbindliches Angebot je nach Projektgröße auf Anfrage.

T · · Systems ·

„FRIENDLY HACKING“ ZUR PRÜFUNG VON SYSTEMEN UND ANWENDUNGEN.

MANUELLE UND SEMI-AUTOMATISCHE PRÜFUNG.

Bei den Tests wenden die Experten eine Kombination aus automatisierten Werkzeugen und manuellen Tests an, um ein Optimum an Effizienz und Aussagekraft zu erzielen. Dabei orientiert sich T-Systems an aktuellen Best Practices für Penetrationstests. Für Webanwendungen sind dies zum Beispiel OWASP (Open Web Application Security Project) und für Systeme und Netze OSSTMM (Open Source Security Testing Methodology Manual). Kunden profitieren automatisch vom aktuellen Stand der Technik und von Innovationen auf diesem Gebiet.

EXPERTEN FÜR ALLE TECHNISCHEN DETAILS.

Je nach Testszenario, Systemumgebung oder Art der technischen Schnittstellen sind bei Penetrationstests unterschiedliche Fähigkeiten und Erfahrungen gefragt. T-Systems verfügt über Experten für diverse Spezialfälle. Zum Beispiel für unterschiedliche Testarten: Während Black-Box-Tests ausschließlich öffentlich verfügbare Informationen als Ausgangspunkt nehmen, greifen White-Box-Tests auch auf Systeminterna wie Netzpläne zurück. Darüber hinaus unterscheiden Penetrationstester zwischen netz- und anwendungsbasierten Checks. Im ersten Fall sucht der Tester nach Systemen im vereinbarten Netz. Er stellt fest, welche Betriebssysteme und Serversoftware zum Einsatz kommen und dokumentiert, wo es Schwachstellen gibt. Im zweiten Fall ist das Ziel, etwa in einer webbasierten Anwendung Fehler zu identifizieren, die zu einer Gefährdung von Vertraulichkeit, Integrität und Verfügbarkeit führen können. Dies beginnt bei Angriffstechniken wie Cross Site Scripting, SQL-Injection oder Privilegien-Eskalation und umfasst ebenso die Prüfung der realisierten Anwendungslogik. In speziellen Bereichen wie Cloud Computing, Mobile Communications und Unified Communication & Collaboration verfügen die Experten von T-Systems über besondere Kompetenzen.

ABSCHLUSSBERICHT MIT MASSNAHMENEMPFEHLUNGEN.

Den konkreten Umfang und die Art der Tests legt T-Systems vorab mit dem Kunden fest. Sie orientieren sich an den Geschäftszielen und den Sicherheitsanforderungen des Kunden. Als Ergebnis der Penetrationstests erstellt T-Systems einen detaillierten Abschlussbericht. Der Bericht führt alle identifizierten Sicherheitslücken auf, priorisiert sie und ergänzt konkrete Empfehlungen für deren Behebung.

ALLGEMEINE TESTMETHODIK.

Penetrationstest Netzwerk	Penetrationstest Anwendungen
Testumfang mit dem Kunden festlegen	
Informationssammlung	
Scannen der Ports	Test des Konfigurationsmanagement
Aufzählung und Bewertung	Authentisierungstest
Schwachstellen-Identifikation/Verifikation	Session-Management-Test
Denial-of-Service-Test (optional)	Autorisierungstest
	Test der Geschäftslogik
	Datenvalidierungstest
	Denial-of-Service-Test (optional)
	Web-Service-Test
	Ajax-Test
Erstellung des Berichts	
Ergebnispräsentation	
Erneuter Test (optional)	

DAS WICHTIGSTE AUF EINEN BLICK.

- Intensiv-Check mit Penetrationstests deckt vorhandene Sicherheitslücken auf
- Testergebnisse dienen als Richtschnur und Basis für nachfolgende Security-Maßnahmen und -Projekte
- Standards und Normen, die eine Überprüfung der Systeme durch Penetrationstests verlangen, werden erfüllt
- Unabhängiger und neutraler Blick von T-Systems als externer ICT-Dienstleister
- Verfügbarkeit von Experten für alle technischen Detailfragen
- Abschlussbericht mit konkreten Maßnahmenempfehlungen

HABEN SIE NOCH FRAGEN?
Internet: www.t-systems.de/security
oder schreiben Sie eine E-Mail an
security-info@t-systems.com

EXPERTENKONTAKT
T-Systems International GmbH
Gerd Enste
Vorgebirgsstr. 49
53119 Bonn

HERAUSGEBER
T-Systems International GmbH
Hahnstraße 43d
60528 Frankfurt
Deutschland