GÖRLITZ

Penetrationstest

Für geprüfte Sicherheit nach Stand der Technik

Die Zahl der Angriffe gegen IT-Systeme hat in den letzten Jahren stetig zugenommen. Besonders über das Internet versuchen Angreifer Zugriff auf Systeme und Daten zu erlangen oder die Verfügbarkeit von Diensten einzuschränken. Sicherlich haben auch Sie Ihr Netzwerk gut gegen Angreifer geschützt. Doch wurde das von unabhängiger Stelle geprüft und bestätigt? Hier hilft Ihnen unser Penetrationstest – kurz Pen-Test – weiter. Mit diesem umfassenden Sicherheitstest für einzelne Rechner oder Netzwerke jeglicher Größe dokumentieren Sie, dass Ihre Vorkehrungen dem Stand der Technik entsprechen. So werden Sie sowohl den Anforderungen einer ISO-27001-Zertifizierung als auch der EU-Datenschutzgrundverordnung (EU-DSGVO) gerecht.

Im Detail

- Dokumentiert die Netzwerksicherheit nach Stand der Technik
- Beim BSI gelistetes Testtool
- Unterschiedlichste Angriffsszenarien mit über 80.000 Tests
- Erfüllt Forderungen aus ISO 27001 bzw. 27002
- Unterstützt „Data Protection by Design“ gemäß EU-DSGVO
- Praxiserprobte Durchführung

Penetrationstest

GÖRLITZ

Wie sicher ist Ihre IT-Infrastruktur?

Die hohe IT-Durchdringung in vielen Bereichen unserer Infrastruktur geht einher mit einer entsprechenden IT-Abhängigkeit. Die unterschiedlichsten Schwachstellen und Sicherheitslücken können aus der Ferne von Angreifern ausgenutzt werden, um einem Unternehmen zu schaden bzw. es auszuspionieren. Daher legen verschiedene gesetzliche und normative Vorgaben besonders bei vernetzten Systemen Wert auf eine entsprechend gute Absicherung der IT-Systeme.

So verweisen etwa die anerkannten Normen ISO 27001 bzw. 27002 im Kapitel „Betriebssicherheit“ darauf, dass Informationen zu technischen Schwachstellen soweit möglich eingeholt und bewertet werden sollen. Penetrationstests werden explizit im Kapitel „Compliance zur Überprüfung der entsprechenden Vorgaben“ empfohlen.

Ähnliche Ansprüche stellt die ab Mai 2018 gültige EU-Datenschutzgrundverordnung. Hier werden in Artikel 25 ausdrücklich Maßnahmen nach Stand der Technik bzw. ein Datenschutz durch Technikgestaltung (data protection by design) gefordert. Mit einem dokumentierten Penetrationstest können Sie nachweisen, dass Ihre Maßnahmen greifen und Sie die Risiken durch externe Angriffe minimiert haben.

Mit dem Pen-Test die Sicherheit weiter erhöhen

Bei einem Penetrationstest werden gezielt Schwachstellen in Ihrer IT-Infrastruktur ermittelt, welche zu einer Minderung der Datensicherheit in Ihrem Unternehmen führen können. Die Art der Sicherheitstests orientiert sich am Gefahrenpotenzial eines gefährdeten Systems, Netzwerks oder einer Anwendung. Daher bedarf es nicht nur eines umfassenden Know-hows in den genannten Bereichen, um einen sicherheitsrelevanten Penetrationstest durchzuführen, sondern auch zusätzlicher Kenntnisse über die durchzuführenden Tests und die korrekte Handhabung der Programme. Wir bei GÖRLITZ haben bereits mehrere dieser Tests durchgeführt und stellen Ihnen unsere Erfahrung jetzt zur Verfügung. Sie profitieren von der Möglichkeit einer zeitnahen Durchführung und können gleichzeitig Ihre Ressourcen in anderen Projekten einsetzen.

Ablauf des Tests

Sie nennen uns die IP-Adressen, die getestet werden sollen und wir führen einen simulierten Angriff durch. Dabei nutzen wir bekannte Schwachstellen, die auch potenzielle Angreifer ausnutzen könnten. Der genaue Zeitpunkt des Tests wird Ihnen nicht mitgeteilt. Sobald uns alle Ergebnisse vorliegen, erhalten Sie eine detaillierte, graphisch aufbereitete Auswertung der verwundbaren Stellen in Ihrem System, unterteilt nach Risikopotenzial. Kritische Sicherheitslücken sind sofort ersichtlich. Bei jedem Punkt werden neben Art und Ort auch die Folgen im Falle eines Angriffs sowie Wege zur Behebung beschrieben. Damit verfügen Sie über eine fundierte Basis, um entsprechende Gegenmaßnahmen umzusetzen und zu dokumentieren. Alle Dokumente zusammen dienen dem Nachweis einer IT-Sicherheit nach Stand der Technik.

Verwendete Tools

Die von uns eingesetzte Software zur Ausführung der Tests ist OpenVAS, das beim Bundesamt für Sicherheit in der Informationstechnik als Empfehlung für Schwachstellen-Scanning und Schwachstellen-Management gelistet ist. Mit über 80.000 (Stand Dezember 2017) sogenannten Network Vulnerability Tests, die laufend aktualisiert und ergänzt werden, können Sie sich auf eine hohe Qualität der Ergebnisse verlassen.

Kostengünstig und zuverlässig

Wir schaffen geprüfte Sicherheit für Ihre Systeme. Als Lösungsanbieter für Energieversorger verfügen wir über langjährige Praxis im Aufbau und der Vernetzung von komplexen IT-Infrastrukturen. Die fachlichen Anforderungen der Energiebranche sind uns vertraut. Darum können wir unser Wissen und unsere Fähigkeiten schnell und kompetent einsetzen. Das spart Zeit und Sie profitieren von einer besonders kostengünstigen Durchführung. Wir bieten Ihnen zwei Optionen an: einen einmaligen Test, um sich z. B. einen Überblick zu verschaffen sowie einen mehrjährigen Vertrag, der zwei Tests pro Jahr beinhaltet. Denn auch die potenziellen Sicherheitsrisiken sind ständigen Veränderungen unterworfen.

Das Gefahrenpotenzial ist dank übersichtlicher Aufbereitung schnell ersichtlich.

(Stand: 07.05.2018, Änderungen vorbehalten)

GÖRLITZ Aktiengesellschaft August-Thyssen-Straße 32 • D-56070 Koblenz
Telefon +49 (0) 261-9285-0 • Telefax +49 (0) 261-9285-190 • E-Mail: info@goerlitz.com • Internet: www.goerlitz.com